Intersection of algebraic plane curves / Some results on the (monic) integer transfinite diameter

Jan Hilmar

Doctor of Philosophy
University of Edinburgh
August 25, 2008

Abstract

Part I discusses the problem of determining the set of intersection points, with corresponding multiplicities, of two algebraic plane curves. We derive an algorithm based on the Euclidean Algorithm for polynomials and show how to use it to find the intersection points of two given curves. We also show that an easy proof of Bézout's Theorem follows. We then discuss how, for curves with rational coefficients, this algorithm can be modified to find the intersection points with coordinates expressed in terms of algebraic extensions of the rational numbers.

Part II deals with the problem of determining the (monic) integer transfinite diameter of a given real interval. We show how this problem relates to the problem of determining the structure of the spectrum of normalised leading coefficients of polynomials with integer coefficients and all roots in the given interval. We then find dense regions of this spectrum for a number of intervals and discuss algorithms for finding discrete subsets of the spectrum for the interval $[0,1]$. This leads to an improvement in the known upper bound for the integer transfinite diameter. Finally, we discuss the connection between the infimum of the spectrum and the monic integer transfinite diameter.

To Richard and Ivan,

and to my parents.

Declaration

I declare that this thesis was composed by myself and that the work contained therein is my own, except where explicitly stated otherwise in the text.

(*Jan Hilmar*)

Contents

Glossary

Part I

$[\boldsymbol{\alpha}]$ Galois Orbit of $\boldsymbol{\alpha}$

$\mathbb{A}K^n$ Affine n-space over the field K

$\partial p, \partial_{x_i} p$ Degree (in x_i) of $p \in K[x_1, \ldots, x_n]$

$\boldsymbol{\Gamma}$ Vandermonde Matrix in γ

$\langle f_1, \ldots, f_n \rangle$ Ideal generated by $f_, \ldots, f_n$

$a \cdot b$ Intersection cycle of a and b

$i_P(f, g)$ Intersection multiplicity of f, g at P

$\overline{K}$ Algebraic closure of K

$K[x_1, \ldots, x_n]$ Polynomial ring in $x_1, \ldots, x_n$ over K

$\langle \mathrm{lt}(I) \rangle$ Ideal generated by the leading coefficients of elements of the polynomial ideal I

$\mathrm{lt}(f)$ Leading term of f

M_n Set of monomials $\boldsymbol{x}^{\boldsymbol{\alpha}}$

$\mathbb{P}K^2$ Projective n-space over the field K

$\mathrm{Res}_{x_i}(f, g)$ Resultant of f, g in x_i

R_P, I_P Localisation of R, I at P

$\mathrm{Syl}_{x_i}(f, g)$ Sylvester Matrix of f, g in x_i

$\boldsymbol{V}(p_1, \ldots, p_n), \boldsymbol{V}(I)$ (Affine) variety generated by $p_1, \ldots, p_n$ / of the ideal I

Part II

$\Delta_n(E), \Delta(E)$ (n^{th}) Fekete constant of $E \subset \mathbb{C}$

$K(x)$ Field of rational functions with coefficients in K

$K_n[x], K_n^*[x]$ Set of (monic) polynomials with coefficients in K and of degree n

$K_n(I), K_n^*(I)$ Set of (monic) polynomials of degree n with coefficients in K and all roots in I

$\mu_n(E)$, $\mu(E)$ (n^{th}) Chebyshev constant of E

$\widetilde{\mu}_n(E)$, $\widetilde{\mu}(E)$ (n^{th}) Chebyshev constant of E, taken over polynomials in $\mathbb{C}^*(E)$

$R(I)$ Set of relations on the interval I

$\|p\|_I$ Supremum norm of p on I

$\mathscr{S}_I$ Spectrum (of normalised leading coefficients) for I

$T_n(x)$, $T_n^*(x)$, $\widetilde{T_n}(x)$ n^{th} Chebyshev polynomial (for $[-1,1]$, $[-2,2]$, $[a,b]$ respectively)

$t(I)$ Transfinite diameter of I

$t_M(I)$ Monic integer transfinite diameter

$t_{\mathbb{Z}}(I)$ Integer transfinite diameter

$\mathscr{U}_d[a,b]$ Set of d-fold rational functions of $[a,b]$ onto itself

Part I

Intersection of Algebraic Plane Curves and Bézout's Theorem

Chapter 1

Introduction

1.1 The Intersection Problem

In basic linear algebra, we learn how to solve simple intersection problems. We might be confronted with finding the intersection points of two lines in the affine plane $\mathbb{A}K^2$ over some field K, defined by equations

$$\begin{aligned} a_1 x + a_2 y &= a_3 \\ b_1 x + b_2 y &= b_3, \end{aligned} \tag{1.1}$$

with $a_i, b_i \in K, 1 \leq i \leq 3$.

The solution to this problem is completely determined by the value of the determinant of the system

$$\begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} = a_1 b_2 - a_2 b_1.$$

If the determinant is 0, the system either has infinitely many solutions (if the lines coincide) or no solutions (if the lines are parallel). If the determinant is nonzero, there exists a unique solution in the affine plane, which can be obtained using Cramer's Rule, for example.

Aside from generalising this to more variables – something that is covered in any basic linear algebra course – one can generalise this problem by increasing the degree of the polynomials involved. While we were trying to find the intersection

points of two given lines above, we might be interested in finding the intersection points of a given pair of bivariate polynomials $p_1(x,y), p_2(x,y) \in K[x,y]$. Even for quadratics, the solution is not nearly as clear as for lines – even attempting to find a generic formula for the number of intersection points appears to be impossible: a pair of circles may intersect in a single point or two points, or may not intersect at all, while an ellipse and a hyperbola might intersect in four points.

The problem has a well-known solution if one of the polynomials involved is a line. If we are asked to find the intersection points of

$$\begin{aligned} a_1 x + a_2 y &= c \\ p(x,y) &= 0 \end{aligned}$$

we can simply eliminate one of the variables using the linear equation to obtain a univariate polynomial $q(x) = p\left(x, \frac{c-a_1 x}{a_2}\right)$, of which we need to find the roots. The Fundamental Theorem of Algebra further tells us that, provided K is algebraically closed and p of degree ∂p, we can expect ∂p roots (counting multiple roots), yielding exactly ∂p intersection points. Using this, we may further find the intersection points of certain classes of polynomials: using the Fundamental Theorem of Algebra once again, we may write any univariate polynomial as a product of linear factors. Thus, if we are given the problem of intersecting

$$\begin{aligned} p(x) &= 0 \\ q(x,y) &= 0 \end{aligned} \tag{1.2}$$

over an algebraically closed field K, we may simply factor $p(x) = a_n \prod_i (x - \alpha_i)$ into (not necessarily unique) linear factors and substitute every factor into $b(x,y)$, yielding the intersection points. In this case, we can then expect $\partial p \partial_y q$ (not necessarily distinct) points over $\mathbb{A}K^2$.

Early pioneers of Algebraic Geometry such as Maclaurin and Euler already observed a "generalisation" of the Fundamental Theorem of Algebra: Given two polynomials $p, q \in K[x,y]$, the algebraic plane curves they define should intersect in $\partial p \partial q$ points in the plane. Clearly, this is not generally the case, as can be seen from the example of two circles intersecting in two points. Nevertheless, Maclaurin conjectured that,

given the correct framework to work in, one should always be able to expect $\partial p \partial q$ points – even though the correct framework was not invented until the advent of projective geometry in the 19th century. Étiénne Bézout famously conjectured this result in his 1779 book *Théorie générale des équations algébraiques*, and gave a proof of the result, failing to address the case where the curves had common points of higher multiplicity. According to [1], a satisfactory proof of the result was not found until 1873 by Georges-Henri Halphen. Nevertheless, Bézout's name is now irrevocably attached to Maclaurin's conjecture, known as Bézout's Theorem.

If we work over the projective field $\mathbb{P}K^2$, our initial problem (1.1) of intersecting two lines has a much nicer solution: Unless the two lines are identical, we always get a unique solution, given by the projective point

$$P = \left(\begin{vmatrix} a_3 & a_2 \\ b_3 & b_2 \end{vmatrix}, \begin{vmatrix} a_1 & a_3 \\ b_1 & b_3 \end{vmatrix}, \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} \right). \tag{1.3}$$

Also, the example of intersecting a univariate polynomial with a bivariate polynomial has a nicer solution when considered projectively. Using the variable z to homogenise the curves, we get

$$p(x,z) = 0$$
$$q(x,y,z) = 0,$$

Factoring $p(x,z) = \lambda \prod_i (x - \alpha_i z)$ into (not necessarily unique) linear factors, we can then substitute the factors $x - \alpha_i z$ into $q(x,y,z)$, to obtain a polynomial

$$q(y,z) = \mu z^k \prod_j (y - \beta_{ij} z) \quad \in K(\alpha_i)[y,z].$$

The difference to (1.2) now is that we are accounting for the "lost" factors $z = 0$, to get exactly $\partial p \partial q$ points, as opposed to the $\partial p \partial_y q$ points in the affine case.

Thus, projective geometry manages to solve some of the mystery of the "lost points" in finding the intersection points of algebraic plane curves. Also, in all of the above special cases, we only get the full number of points conjectured by Maclaurin if we count multiple points – equvialent to the fact that the Fundamental

Theorem of Algebra only gives the correct number of roots if we count roots with their multiplicities.

This is the second issue encountered by early workers of Algebraic Geometry: while it is relatively clear what is meant by multiplicity of a root in the univariate case – one simply looks at the exponent of the factor in the factorisation of the polynomial – this is far from clear in the multivariate case and a rigorous definition of intersection multiplicity was not obtained until the 19th century. Given a suitable definition of intersection multiplicity, however, one can phrase Bézout's Theorem rigorously:

Theorem 1.1.1 (Bézout's Theorem)**.** *Let $a, b \in K[x, y, z]$ be homogeneous polynomials with* $\gcd(a, b) = 1$ *and K be an algebraically closed field. Then the algebraic curves defined by a and b intersect in $\partial a \partial b$ points in $\mathbb{P}K^2$, counting multiplicities.*

1.2 Remarks on Notation

In the following discussion, we will slightly abuse notation by identifying an algebraic curve with the polynomial defining it. Thus, we will be talking about an "algebraic curve" $y^2 - x^3$, when we actually mean the variety $\boldsymbol{V}(y^2 - x^3)$. By the degree of an algebraic curve, we always mean the degree of its defining equation and will let $\partial a, \partial_x a, \partial_y a$ denote the total degree, x-degree and y-degree of $a \in K[x, y]$, respectively.

Throughout the text, $\overline{K}$ will denote the algebraic closure of the field K.

Chapter 2

Methods for finding intersection points

Just as Gaussian Elimination or Cramer's Rule offer methods for solving a system of linear equations, there are various methods that can be employed to solve a system of general polynomial equations. The two most common methods are the use of resultants and Gröbner Bases. We will discuss these methods in the following sections and show their advantages and drawbacks.

2.1 Resultants

We start with some necessary and sufficient conditions for two univariate polynomials to have a common root. This will then lead to the definition of the resultant $\mathrm{Res}_x(f,g)$ of univariate polynomials $f,g \in K[x]$ which can subsequently be used to find the intersection points of two given algebraic curves over $\mathbb{P}K^2$.

We start with the following lemma from [11]:

Lemma 2.1.1. *Let $f,g \in K[x]$. Then f and g have a common component if and only if there exist nonzero $a,b \in K[x]$ with $\partial a < \partial g, \partial b < \partial f$ such that*

$$af + bg = 0$$

Proof. Suppose that $\gcd(f,g) = m$ and write $f = f'm, g = g'm$. Then

$$g'f - f'g = g'f'm - f'g'm = 0$$

so that we may choose $a = g', b = -f'$.

Suppose that, for $a, b \in K[x]$ as in the assumptions, $af + bg = 0$, but $\gcd(f,g) = 1$. Then there exist $\widetilde{a}, \widetilde{b} \in K[x]$ with $1 = \widetilde{a}f + \widetilde{b}g$, so that

$$\begin{aligned} b &= \widetilde{a}bf + \widetilde{b}bg \\ &= f(\widetilde{a}b - \widetilde{b}a) \end{aligned}$$

contradicting that $\partial b < \partial f$. □

If we now use explicit expressions for the polynomials involved, setting

$$\begin{aligned} f(x) &= a_n x^n + \cdots + a_0 \\ g(x) &= b_m x^m + \cdots + b_0 \\ a(x) &= c_{m-1} x^{m-1} + \cdots + c_0 \\ b(x) &= d_{n-1} x^{n-1} + \cdots + d_0 \end{aligned} \tag{2.1}$$

we may rewrite $af + bg = 0$ as the matrix equation

$$\begin{bmatrix} a_n & 0 & 0 & \cdots & 0 & 0 & 0 \\ a_{n-1} & a_n & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \vdots & 0 & a_0 & a_1 \\ 0 & 0 & 0 & \vdots & 0 & 0 & a_0 \\ b_m & 0 & 0 & \cdots & 0 & 0 & 0 \\ b_{m-1} & b_m & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \vdots & 0 & b_0 & b_1 \\ 0 & 0 & 0 & \vdots & 0 & 0 & b_0 \end{bmatrix} \begin{bmatrix} c_{m-1} \\ c_{m-2} \\ \vdots \\ c_1 \\ c_0 \\ d_{n-1} \\ d_{n-2} \\ \vdots \\ d_1 \\ d_0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{bmatrix} \tag{2.2}$$

This coefficient matrix is the so-called Sylvester Matrix $\mathrm{Syl}_x(f,g)$ of the polynomials.

As we know from basic linear algebra, the system has a nontrivial solution if and only if the determinant of the coefficient matrix is zero. We thus make the following definition:

Definition 2.1.1. Let $f, g \in K[x]$. The Resultant $\mathrm{Res}_x(f,g)$ of f and g is defined to be the determinant of $\mathrm{Syl}_x(f,g)$.

Clearly, f and g have a common root if and only if $\mathrm{Res}_x(f,g) = 0$.

The Resultant also has an alternative representation in terms of the roots of the polynomials.

Theorem 2.1.1. *Let $f, g \in K[x]$ have factorisations $f(x) = a_n \prod_i^n (x-\alpha_i)$, $g(x) = b_m \prod_j^m (x-\beta_j)$ over $\overline{K}$. Then*

$$\mathrm{Res}_x(f,g) = a_n^m b_m^n \prod_{\substack{1\le i\le n \\ 1\le j\le m}} (\alpha_i - \beta_j) \tag{2.3}$$

Proof. Clearly, the resultant is a polynomial in the coefficients of f and g, as can be seen by simply expanding the determinant. Further, consider $\mathrm{Res}_x(f,g) = r(a_0, a_1, \ldots, a_n)$

and, for $\lambda \neq 0 \in K$, look at $r(\lambda a_0, \lambda a_1, \ldots, \lambda a_n)$. By definition, this equals

$$\det \begin{bmatrix} \lambda a_n & \cdots & 0 & \cdots & 0 \\ \lambda a_{n-1} & \lambda a_n & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & \cdots & \lambda a_0 \\ b_m & \cdots & 0 & \cdots & 0 \\ b_{m-1} & b_m & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & \cdots & b_0 \end{bmatrix} = \det \begin{bmatrix} a_n & \cdots & 0 & \cdots & 0 \\ \lambda a_{n-1} & \lambda a_n & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & \cdots & \lambda a_0 \\ b_m & \cdots & 0 & \cdots & 0 \\ b_{m-1} & b_m & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & \cdots & b_0 \end{bmatrix}$$

$$= \lambda^m \det \begin{bmatrix} a_n & \cdots & 0 & \cdots & 0 \\ a_{n-1} & a_n & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & \cdots & a_0 \\ b_m & \cdots & 0 & \cdots & 0 \\ b_{m-1} & b_m & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & \cdots & b_0 \end{bmatrix} = \lambda^m r(a_0, a_1, \ldots, a_n),$$

showing that $\mathrm{Res}_x(f,g) = r(a_0, a_1, \ldots, a_n)$ is a homogeneous polynomial of degree m. The same argument applied to the coefficients of $g(x)$ shows that the resultant is further a homogeneous polynomial $\widetilde{r}(b_0, b_1 \ldots, b_m)$ of degree n in the b_i, $1 \leq i \leq m$. Now, using homogeneity, we may write

$$r(a_0, a_1 \ldots, a_n) = a_n^m r\left(\frac{a_0}{a_n}, \frac{a_1}{a_n}, \ldots, 1\right)$$
$$\widetilde{r}(b_0, b_1 \ldots, b_m) = b_m^n \widetilde{r}\left(\frac{b_0}{b_m}, \frac{b_1}{b_m}, \ldots, 1\right).$$

Now, $\frac{a_i}{a_n} = (-1)^{n-i} s_{n-i}(\alpha_1, \ldots, \alpha_n)$ and $\frac{b_j}{b_m} = (-1)^{m-j} s_{m-j\,j}(\beta_1, \ldots, \beta_m)$ are the fundamental symmetric polynomials in the roots of $f(x)$ and $g(x)$, respectively. Thus, r and $\widetilde{r}$, homogeneous polynomials in the fundamental symmetric polynomials, are symmetric in $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m$, themselves.

Note now that, if for some i, j, $\alpha_i = \beta_j$, the resultant vanishes by definition. Thus,

$\alpha_i - \beta_j$ is a factor of $\mathrm{Res}_x(f,g)$. Consequently, the monic part of the resultant is divisible by the product

$$\prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j),$$

a symmetric polynomial in the α_i and β_j. Seeing that the resultant, viewed as a symmetric polynomial in the roots of $f(x)$, is of degree at most mn and the above product is of degree mn in the α_i, we get

$$\mathrm{Res}_x(f,g) = a_n^m b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j). \qquad \square$$

The resultant has a few important properties worth noting:

Proposition 2.1.1. *Let $f, g \in K[x]$ as above. Then*

(a) $\mathrm{Res}_x(f,g) = a_n^m \prod_{i=1}^{n} g(\alpha_i) = b_m^n \prod_{j=1}^{m} f(\beta_j)$

(b) $\mathrm{Res}_x(f,gh) = \mathrm{Res}_x(f,g)\,\mathrm{Res}_x(f,h)$ *for any* $h \in K[x]$.

(c) If $f = qg + r$, $\mathrm{Res}_x(f,g) = b_m^{n-\partial r}\,\mathrm{Res}_x(g,r)$.

(d) $\mathrm{Res}_x(f,g)$ *is a polynomial in the coefficients of* f *and* g.

Proof. (a) comes straight from the expression of the resultant in (2.3), as does (b). To prove (c), consider

$$\begin{aligned}
\mathrm{Res}_x(f,g) &= a_m^n \prod_{j=1}^{m} f(\beta_j) \\
&= a_m^n \prod_{j=1}^{m} \big(q(\beta_j)g(\beta_j) + r(\beta_j)\big) \\
&= a_m^n \prod_{j=1}^{m} r(\beta_j) \\
&= a_m^{n-\partial r}\,\mathrm{Res}_x(g,r).
\end{aligned}$$

Part (d) follows straight from Definition 2.1.1. $\square$

Part (c) yields an efficient algorithm for computing the resultant, based on the Euclidean Algorithm.

If we are now given two bivariate polynomials $f(x,y), g(x,y)$, we may write them as

$$f(x,y) = \sum_{i=0}^{\partial_x f} f_i(y)x^i$$
$$g(x,y) = \sum_{i=0}^{\partial_x g} g_i(y)x^i,$$

considering them as polynomials in x with coefficients in $K[y]$. Formally calculating the x-resultant $\mathrm{Res}_x(f,g)$ will then yield a polynomial in y. Since a necessary and sufficient condition for the polynomials to have a common root in x is that the x-resultant is zero, the roots of this polynomial yield the y-coordinates of the intersection points of f and g. The corresponding x-coordinates may be obtained by substituting the solutions of $\mathrm{Res}_x(f,g) = 0$ into either $f(x,y)$ or $g(x,y)$ and finding the roots of the resulting univariate polynomial. A simple example of this is the following: Let $K = \mathbb{Q}$ and consider the polynomials

$$f(x,y) = x^2 + y^2 + 1$$
$$g(x,y) = xy.$$

The resultant is easily computed to be

$$\mathrm{Res}_x(f,g) = y^2(y^2+1).$$

If we now take the roots $y = 0$ and $y = \pm i$ and substitute them back into $f(x,y)$, we get the corresponding intersection points $(\pm i, 0)$ and $(0, \pm i)$.

Thus, using the resultant gives an efficient algorithm for finding the intersection points of two algebraic curves with no common component. We could also use the resultant to attempt to give a definition of intersection multiplicity: If we took two projective curves, defined by homogeneous polynomials $f(x,y,z), g(x,y,z)$, the x-resultant will be a homogeneous polynomial in $K[y,z]$ of the form

$$\mathrm{Res}_x(f,g) = r_l \prod_i (y - \gamma_i z)^{k_i}.$$

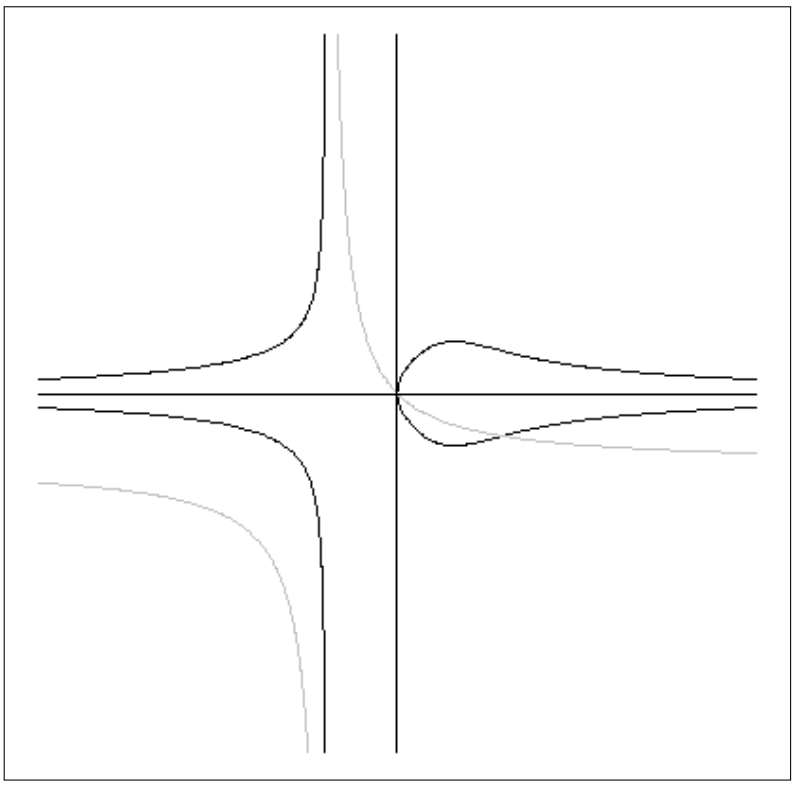

Figure 2.1: Affine versions of f (black) and g (grey) in (2.4).

It is tempting to define the multiplicity of intersection at the point $(x_i, \gamma_i, 1)$ to be the multiplicity k_i of the root $y = \gamma_i z$ in $\mathrm{Res}_x(f,g)$. This does not always work, however, as the following example shows.

Let $K = \mathbb{C}$ and

$$\begin{aligned} f(x,y,z) &= x^3y^2 - xz^4 + y^2z^3 \\ g(x,y,z) &= xy + xz + yz. \end{aligned} \tag{2.4}$$

If we compute the x-resultant, we get

$$\mathrm{Res}_x(f,g) = yz^4(3y^3 + 4y^2z + 3z^2y + z^3),$$

a polynomial of degree 8. Seeing that Bézout's Theorem dictates that f and g should have 10 common points, the multiplicities of intersection cannot be correct in this case. If we attempted to get around this problem by finding the $y-$ and $z-$ resultants,

we would get

$$\begin{aligned}\mathrm{Res}_y(f,g) &= -xz^2(x^2z^2 + xz^3 + z^4 - x^4)\\ \mathrm{Res}_z(f,g) &= -x^4y^2(3y^3 + 5xy^2 + 4x^2y + x^3),\end{aligned}$$

polynomials of degrees 7 and 9, respectively – neither of which can give the correct intersection multiplicities, by Bézout's Theorem. This is due to the following:

Lemma 2.1.2. *Let $f, g \in K[x,y,z]$ be homogeneous polynomials with no common component. Then the x-resultant is a homogeneous polynomial in y and z, of degree*

$$\partial_x f \partial_x g + (\partial f - \partial_x f)\partial_x g + (\partial g - \partial_x g)\partial_x f \leq \partial f \partial g, \tag{2.5}$$

with equality if and only if $P = (1,0,0)$ does not lie on both curves.

Proof. Suppose that

$$\begin{aligned}f(x,y,z) &= \sum_{i=0}^{\partial_x f} a_i(y,z)x^i\\ g(x,y,z) &= \sum_{i=0}^{\partial_x g} b_i(y,z)x^i\end{aligned}$$

We know from Theorem 2.1.1 that the x-resultant is a polynomial of degree $\partial_x f \partial_x g$ in the roots of f and g, when viewed as polynomials in x, multiplied by the term $a_{\partial_x f}(y,z)^{\partial_x g} b_{\partial_x g}(y,z)^{\partial_x f}$, which is of degree $(\partial f - \partial_x f)\partial_x g + (\partial g - \partial_x g)\partial_x f$. Adding the degrees gives (2.5).

Suppose that, without loss of generality, $f(1,0,0) \neq 0$. Then $\partial_x f = \partial f$, and equation (2.5) turns into $\partial f \partial g$. If, on the other hand, $\partial f \partial g = \partial \mathrm{Res}_x(f,g)$, then we have

$$\begin{aligned}\partial f \partial g - \partial \mathrm{Res}_x(f,g) =& \partial f \partial g - (\partial_x f \partial_x g + \partial_x f(\partial g - \partial_x g) + \partial_x g(\partial f - \partial_x f))\\ =& (\partial f - \partial_x f)(\partial g - \partial_x g) = 0,\end{aligned}$$

so that either $\partial_x f = \partial f$, or $\partial_x g = \partial g$. This only happens if one of f, g is nonzero at $(1,0,0)$. □

The problem can be solved by first applying a suitable change of coordinates to the curves to make sure at least one of $(1,0,0),(0,1,0),(0,0,1)$ does not lie on both curves - in which case we say that the curves are in *good position*. We can then use the $x-$, $y-$ or $z-$ resultant respectively to find the intersection points. The resultant will be a polynomial of degree $\partial f \partial g$ and the intersection multiplicity of an intersection point can then be defined to be the exponent of the corresponding root in the factorisation of the resultant. That this indeed gives the correct intersection multiplicity will be shown in Section 3.1.

2.2 Gröbner Bases

While the use of resultants is a rather basic algebraic idea, one can approach the problem of finding the common solutions to a system of polynomial equations $f_1 = 0, \ldots, f_n = 0$ over $K[x_1, \ldots, x_n]$ more systematically, using some basic algebraic geometry.

Suppose we are given a set of polynomials $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$. We will start by working over the affine plane $\mathbb{A}K^n$ and then extend the ideas to the projective plane. If we consider the variety $\boldsymbol{V}(f_1, \ldots, f_n) = \{P \in \mathbb{A}K^n \mid f_1(P) = \cdots = f_m(P) = 0\}$, it is clear that any zero of a polynomial of the form

$$g = \sum_{i=1}^{m} a_i f_i,\ a_i \in K[x_1, \ldots, x_n]$$

will also be in the variety. Thus, the variety is actually an object dependent on the ideal $I = \langle f_1, \ldots, f_m \rangle$ in $K[x_1, \ldots, x_n]$ generated by the polynomials, rather than the polynomials themselves. Working algebraically, it is therefore natural to study ideals in the ring $K[x_1, \ldots, x_n]$.

If $n = 1$, the ideals are easily classified. For any field K, the polynomial ring $K[x]$ is a principal ideal domain, generated by the greatest common divisor of the polynomials. This is directly due to the existence of a degree function on the ring of polynomials and the division algorithm that uses the degree function. Unfortunately, the same does not hold in more than one variable. The ideal $I = \langle x, y \rangle \subset K[x, y]$ cannot be principal, as any generator for the ideal would have to divide both x and y.

Of course, this makes the ring $K[x_1,\dots,x_n]$ a lot harder to deal with when $n>1$. It does, however, have a rather nice property. We make the following definition:

Definition 2.2.1. A ring K is called **Noetherian** if for every increasing chain of nested ideals

$$I_1 \subset I_2 \subset \cdots,$$

there exists some $N \in \mathbb{N}$ with $I_n = I_N$ for $n > N$.

Clearly, fields are trivially Noetherian, since they do not have any proper ideals. That polynomial rings satisfy this property is essentially a corollary of the following theorem, which is the essence of Hilbert's Basis Theorem:

Theorem 2.2.1. *Let R be a Noetherian Ring. Then $R[x]$ is Noetherian.*

Proof. Let R be Noetherian and choose f_1 arbitrary in $R[x]$. Construct a sequence of ideals $I_i, i = 1,\dots$ in the following manner: given $I_i = \langle f_1,\dots,f_i\rangle$, let $I_{i+1} = \langle f_1,\dots,f_i,f_{i+1}\rangle$ with f_{i+1} of minimal degree in $R[x]\setminus I_i$. We get a chain of ideals

$$I_1 \subset I_2 \subset \cdots$$

Consider now the leading coefficient a_i of f_i. If we let $J_i = \langle a_1,\dots,a_i\rangle$, we get a corresponding sequence of ideals

$$J_1 \subset J_2 \subset \cdots$$

Since R is Noetherian, we have some $N \in \mathbb{N}$ with $J_N = J_{N+1} = \cdots$, so $a_{N+1} \in J_N$. Thus, there exist $u_1, u_2, \dots, u_N$ with $a_{N+1} = \sum_{i=1}^{N} u_i a_i$. Let $g = \sum_{i=1}^{N} u_i f_i x^{\partial f_{N+1} - \partial f_i}$ be the corresponding polynomial and note that it has leading coefficient a_{N+1} and is of degree ∂f_{N+1}, so that $f_{N+1} - g$ is of degree less than ∂f_{N+1}, so must be in I_i and, as such, generated by the $f_1,\dots,f_N$. But then f_{N+1} is as well and $I_N = I_{N+1}$. □

Using a simple recursive argument, this shows that $K[x_1,\dots,x_n]$ is Noetherian for any $n \in \mathbb{N}$. An important consequence (and actually equivalent alternative defintition of Noetherian) that comes out of this theorem is that ideals in a Noetherian ring are

always finitely generated – they are generated by a finite set of elements of the ideal. This is also known as Hilbert's Basis Theorem.

Now, if we are given an ideal $I \subset K[x_1, \ldots, x_n]$ in terms of its generating set, we may ask whether a given polynomial f is a member of the ideal. In one variable, the answer to this is simple: since $K[x]$ is a principal ideal domain generated by the greatest common divisor of the elements in the ideal, it is enough to check whether the given polynomial is a multiple of the generator. An efficient algorithm for checking this is given by the Division Algorithm. The Division Algorithm givens a reduction of a polynomial to a remainder, using a generator for the ideal. If the remainder is zero, the polynomial in question is an element of the ideal. Given the ideal $I = \langle x^2 - 1 \rangle \subset K[x]$ and the polynomial $f(x) = x^3 + 2x - 1$, for example, we use the division algorithm to write

$$x^3 + 2x - 1 = (x^2 - 1)x + 3x - 1$$

and see immediately that f is not an element of the ideal, as it has remainder $r(x) = 3x - 1$ upon division by $x^2 - 1$.

We can use a similar procedure in the multivariate case: Given an ideal $I = \langle f_1, \ldots, f_m \rangle \subset K[x_1, \ldots, x_n]$, and a polynomial g, we can attempt to write

$$g = a_1 f_1 + \ldots + a_m f_m + r. \tag{2.6}$$

If we manage to find such an expression such that $r = 0$, we get that $g \in I$. To do this, we may systematically add multiples of the generators $f_1, \ldots, f_m$ of the ideal to the given polynomial. We may start with f_1 (relabelling the generators if necessary), and call this process "reducing g using f_1". Writing

$$g \to_{f_1} g_1,$$

we mean that, for some $h \in K[x_1, \ldots, x_n]$, $g_1 = g + hf_1$. We repeat this, getting a

sequence

$$g \to_{f_1} g_1 \to_{f_2} \cdots \to_{f_m} r$$

(renumbering the generators f_i if necessary) until we produce a polynomial r that can no longer be reduced using generators, at which point we have produced the r in (2.6).

Consider the following example, taken from [11]: Let $f_1 = xy + 1$, $f_2 = y^2 - 1$, $I = \langle f_1, f_2 \rangle$ and let $g = xy^2 - x$. Using f_1, we can eliminate the xy^2 term by taking $g_1 = g - yf_1 = -x - y$. Since the total degree of g_1 is less than the total degree of f_2, we may be led to believe that the remainder is $-x - y$ and that g is not an element of the ideal.

If we repeat the same process using f_2 first to get $g_1 = g - xf_2 = 0$, we now get a remainder of 0, proving that g is indeed in the ideal. Thus, this procedure has a major drawback: the order in which we use elements of the ideal matters – the remainder is consequently not unique!

To attempt to solve this problem, we first need to make the process of "reducing" polynomials using basis elements rigorous. First, we define a **monomial** to be a polynomial of the form $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, where $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{N}$, which we will write in shorthand notation as $\boldsymbol{x}^{\boldsymbol{\alpha}}$. Let M_n denote the set of monomials in the variables $x_1, \ldots, x_n$.

Definition 2.2.2. A **monomial order** $>$ is a relation on M_n with the following properties:

- For $\boldsymbol{x}^{\boldsymbol{\alpha}}, \boldsymbol{x}^{\boldsymbol{\beta}} \in M_n$, exactly one of $\boldsymbol{x}^{\boldsymbol{\alpha}} > \boldsymbol{x}^{\boldsymbol{\beta}}$, $\boldsymbol{x}^{\boldsymbol{\beta}} > \boldsymbol{x}^{\boldsymbol{\alpha}}$ or $\boldsymbol{x}^{\boldsymbol{\alpha}} = \boldsymbol{x}^{\boldsymbol{\beta}}$ holds.
- $\boldsymbol{x}^{\boldsymbol{\alpha}} > 1$ for all $\boldsymbol{x}^{\boldsymbol{\alpha}} \in M_n$.
- If $\boldsymbol{x}^{\boldsymbol{\alpha}} > \boldsymbol{x}^{\boldsymbol{\beta}}$, then $\boldsymbol{x}^{\boldsymbol{\alpha}}\boldsymbol{x}^{\boldsymbol{\gamma}} > \boldsymbol{x}^{\boldsymbol{\beta}}\boldsymbol{x}^{\boldsymbol{\gamma}}$ for any $\boldsymbol{x}^{\boldsymbol{\gamma}} \in M_n$.

A simple example of a monomial ordering is the so-called pure lexicographical ordering (*plex*). Here, we define an order on the variables first (e.g. $x_1 > x_2 > x_3 > \cdots > x_n$) and then compare powers within a variable. More precisely, $\boldsymbol{x}^{\boldsymbol{\alpha}} >_{plex} \boldsymbol{x}^{\boldsymbol{\beta}}$ if the leftmost non-zero entry in the vector $\boldsymbol{\alpha} - \boldsymbol{\beta}$ is positive. We will let $plex(x_1, x_2, \ldots, x_n)$ denote the pure lexicographical ordering with $x_1 > x_2 > \ldots > x_n$.

There are a number of monomial orderings (see [11] for additional examples), but *plex* is the only one we need for our purposes.

Once we fix a monomial ordering on M_n, we can define the leading term $\mathrm{lt}(f)$ of a polynomial $f \in K[x_1, \ldots, x_n]$ to be the term of maximal order of the polynomial. Under $plex(x, y)$, the polynomial $f = 2x^2y + y^5x$ has leading term $2x^2y$, while it has leading term y^5x under $plex(y, x)$.

One can then make the algorithm sketched earlier more systematic: Given a polynomial g and an ideal $I = \langle f_1, \ldots, f_n \rangle$, we take an element f of I such that $\mathrm{lt}(f_i) \mid \mathrm{lt}(g)$ and use it to eliminate the leading term of g, possibly introducing additional terms of lower order. If at any point, no such $f \in I$ exists, we have reached the remainder.

It would of course be very useful to be able to do these reductions using basis elements only. For this purpose, we will make the following definition. For a given ideal I, let $\langle \mathrm{lt}(I) \rangle$ denote the ideal generated by the leading coefficients of elements of I.

Definition 2.2.3. Let $I \subset K[x_1, \ldots, x_n]$ be an ideal. A Gröbner Basis $G = \{g_1, \ldots, g_m\}$ for I is a basis such that $\langle \mathrm{lt}(g_1), \mathrm{lt}(g_2), \ldots, \mathrm{lt}(g_m) \rangle = \langle \mathrm{lt}(I) \rangle$.

When making such a definition, it is important to prove that such objects actually exist. Before we can prove this, we need a short Lemma about monomial ideals:

Lemma 2.2.1. *Let I be an ideal of $K[x_1, \ldots, x_n]$. Then the following are equivalent:*

1. *I is a monomial ideal*
2. *$f \in I \iff$ every term of f lies in I*

Proof. To show that (1) $\implies$ (2), let I be a monomial ideal. Then, if $f \in I$, it can be reduced to 0 using elements $g_1, \ldots, g_n \in I$:

$$f \to_{g_1} f_1 \cdots \to_{g_n} 0,$$

relabelling the g_i where necessary. As the g_i are all monomials, we are removing a single term from f at every step, which consequently lies in I (as it is a multiple of a generator). The converse of part (2) is trivial.

To show that (2) $\Longrightarrow$ (1), we may use Hilbert's Basis Theorem to find a basis $\{f_1,\ldots,f_m\}$ for I. Writing now $f_i = \sum_{j=1}^{n_i} f_{ij}$, as a sum of monomials, we know that every term f_{ij} lies in I. Thus, $I = \langle f_{ij}\rangle_{\substack{1\le j\le n_i\\ 1\le i\le m}}$ is a monomial ideal. □

Consider now $\langle \mathrm{lt}(I)\rangle$. If $g \in \langle \mathrm{lt}(I)\rangle$, then $g = \sum_{i=1}^{d} a_i \,\mathrm{lt}(f_i), a_i, f_i \in K[x_1,\ldots,x_n]$, so that every term of g lies in $\langle \mathrm{lt}(I)\rangle$. It follows that $\langle \mathrm{lt}(I)\rangle$ is a monomial ideal. Using this, we can prove the following:

Theorem 2.2.2. *Fix a monomial ordering on M_n and let I be an ideal in $K[x_1,\ldots,x_n]$. Then there exists a Gröbner Basis G for I.*

Proof. Consider the monomial ideal $\langle \mathrm{lt}(I)\rangle$ and choose a set of elements $G = \{g_1,\ldots,g_m\} \subset I$ such that $\langle g_1,\ldots,g_m\rangle = \langle \mathrm{lt}(I)\rangle$, where $g_1,\ldots,g_m$ are monomials.

To show that G is a basis for I, note that if $f \in I$, then there is some element g_i of G such that $g_i \mid \mathrm{lt}(f)$. Repeating this for $f - \mathrm{lt}(f) \in I$, we see that its leading term is divisible by some g_j. Repeating this process, we can eliminate all terms of f using elements of G, showing that $f \in \langle G\rangle$. □

Knowing that Gröbner Bases exist, it is convenient to be able to compute them. Such algorithms exist, but will not be covered here, as this exceeds the scope of what we need. An outline of the basic algorithm can be found in any text on Gröbner Bases, such as [2].

To show how Gröbner Bases can be used to solve systems of polynomial equations, we define the i^{th} **elimination ideal** I_i by

$$I_i = I \cap K[x_{i+1},\ldots,x_n].$$

This is essentially an ideal eliminating the first i variables, hence the name. Gröbner Bases, when computed with respect to $plex(x_1,\ldots,x_n)$, behave very well with respect to elimination ideals:

Lemma 2.2.2. *Let $I \subset K[x_1,\ldots,x_n]$ be an ideal, G a Gröbner Basis for I using $plex(x_1,\ldots,x_n)$. Then the set*

$$G_i = G \cap K[x_{i+1},\ldots,x_n]$$

is a Gröbner Basis for I_i.

Proof. Let $G = \{g_1, \dots, g_k\}$, and $f \in I_i$. Then, relabelling the elements of G if necessary, $\mathrm{lt}(f)$ is divisible by g_1, which we can use to eliminate $\mathrm{lt}(f)$. Repeating this process, we get a reduction

$$f \to_{g_j} f_1 \to_{g_2} \cdots \to_{g_k} 0$$

using only elements from G_i, as $f \in K[x_{i+1}, \dots, x_n]$. □

The simplicity of the proof of this argument is a recurrent theme in the theory of Gröbner Bases: while the definitions seem complicated at times, the entire theory is very natural and proofs fall into place without much effort. Let us illustrate the power of the above result on an example:

Suppose we want to find the variety $\boldsymbol{V}(f_1, f_2)$, where $f_1(x,y) = y^2 - x^3$, $f_2(x,y) = x^4 + x^2y^2 \in K[x,y]$. Using $plex(x,y)$, we get a Gröbner Basis for the ideal $I = \langle f_1, f_2 \rangle$

$$G = \{y^4 + y^6, y^2x - y^4, -y^2 + x^3\}$$

so that $G_1 = \{y^4(y^2+1)\}$. To find the intersection points, we simply find the roots of the univariate polynomial $y^4(y^2+1)$ and substitute these into f_1 or f_2 to obtain the corresponding x-values, similar to the procedure with resultants.

To see how resultants relate to Gröbner Bases, we need the following lemma:

Lemma 2.2.3. *Let $f, g \in K[x,y,z]$ have no common component. Then, if $(1,0,0)$ does not lie on f and g, $\mathrm{Res}_x(f,g) \in \langle f, g \rangle$.*

Proof. We will provide a purely algebraic proof following [11], using only basic linear algebra.

Let a, b be as in (2.1) and consider the equation $\widetilde{a}f + \widetilde{b}g = 1$. Writing this as in (2.2) as a matrix equation with coefficients in $K[y,z]$ and coefficient matrix D, we see that $\det D = \mathrm{Res}_x(f,g)$. Noting that $D \neq 0$ (the curves have no common component),we may use Cramer's Rule to get a solution of the form $\boldsymbol{c} = (c_1, \dots, c_{m+n})$ with $c_i = \frac{D_i}{D}$.

Here, D_i is the determinant of a matrix with entries in $K[y,z]$. Thus, we may write

$$1 = \widetilde{a}f + \widetilde{b}g = \frac{a}{\mathrm{Res}_x(f,g)}f + \frac{b}{\mathrm{Res}_x(f,g)}g$$

where $a, b \in K[x,y,z]$.

Clearing denominators, we get the result. □

The connection between resultants and Gröbner Bases using purely lexicographical order is quite simple: Over $K[x,y]$, G_1 will be a basis for $I_1 = I \cap K[y]$. Further, as an ideal over a univariate polynomial ring, I_1 is principal, so $I_1 = \langle g \rangle$. $\mathrm{Res}_x(f,g) \in I \cap K[y] = I_1$ is consequently a multiple of g.

Since our discussion focuses on Bézout's Theorem, we need to mention a few facts about how to extend the notion of Gröbner Bases to projective varieties. The corresponding algebraic objects in this case are the so-called homogeneous ideals:

Definition 2.2.4. An ideal $I \subset K[x_1,\ldots,x_n,x_{n+1}]$ is a **homogeneous ideal** if $I = \langle f_1,\ldots,f_m \rangle$ where the f_i are homogeneous polynomials.

Note that we do not require that the generators have the same degree – clearly, the elements of a homogeneous ideal are not homogeneous polynomials themselves. Instead, we consider I as an ideal of the ring $K[x_1,\ldots,x_n,x_{n+1}]$. We still get the correspondence between and ideal and its variety, as every element of the form $h = \sum_i h_i$ will vanish at all points of the variety $\boldsymbol{V}(h_1,\ldots,h_m)$.

Let $f \in K[x_1,\ldots,x_n,x_{n+1}]$ be a homogeneous polynomial. We can write

$$f(x_1,\ldots,x_n,x_{n+1}) = \sum_{i=0}^{d} f_i(x_1,\ldots,x_n,x_{n+1})$$

where $\partial f_i = i$. We will call f_i the i^{th} *homogeneous component* of f.

Homogeneous ideals have a very nice property (and alternative characterisation) in terms of the homogeneous components of their elements:

Lemma 2.2.4. *An ideal I is homogeneous if and only if, for every $f \in I$, every homogeneous component f_i of f also lies in I.*

Proof. Let $I = \langle g_1, \ldots, g_m \rangle$ be a homogeneous ideal, and let

$$f = \sum_{i=0}^{m} a_i g_i.$$

Now we write $a_i = \sum_{j=0}^{d_i} a_{ij}$ as the sum of its homogeneous components in $K[x_1, \ldots, x_{n+1}]$. Rewriting, we get

$$\sum_{k=0}^{d} f_i = \sum_{j=0}^{d_1} a_{1j} g_1 + \ldots + \sum_{j=0}^{d_m} a_{mj} g_m.$$

Comparing terms on both sides, we see that the term f_k of total degree k will be of the form $f_k = b_1 g_1 + \ldots + b_m g_m$ for $b_i \in K[x_1, \ldots, x_m]$, so is in I

To prove the converse, let I be a homogeneous ideal. Then $I = \langle g_1, \ldots, g_m \rangle$ by Hilbert's Basis Theorem. Let $g_i = \sum_j g_{ij}$, where the g_{ij} are homogeneous. Then $I = \langle g_{ij} \rangle$ is generated by homogeneous polynomials, and thus a homogeneous ideal. □

Following the second part of the proof, it is easy to see that a homogeneous ideal will always have a homogeneous Gröbner Basis with respect to a given monomial order. If $G = \{g_1, \ldots, g_k\}$ is a Gröbner basis for I, then the set $G' = \{g_{ij}\}$ of homogeneous components of the elements of G is a homogeneous Gröbner basis for I (as $\{lt(g_i) : g_i \in G\} \subset \{lt(g_{ij} : g_{ij} \in G'\})$.

Thus, Gröbner Bases give a very nice algebraic way of solving systems of equations. However, since the method works with the ideal generated by the polynomials rather than with the polynomials themselves, Gröbner Bases do not allow us to conclude anything about the multiplicity of a point on a variety.

Chapter 3

Intersecting algebraic curves using the Euclidean Algorithm

In the Introduction, we saw that the definition of intersection multiplicity of two algebraic curves plays an important role, especially in light of Bézout's Theorem. Using resultants, one can define intersection multiplicity – yet this definition only works for curves in "good position". In this section, we will introduce a rigorous definition of intersection multiplicity and use it, together with the Euclidean algorithm for polynomials, to derive an algorithm for finding the intersection points, with their correct multiplicities, of two given algebraic curves.

3.1 Multiplicity of Intersection and Intersection Cycles of Curves

In this section, we will motivate a definition of intersection multiplicity and outline and prove some important properties of this multiplicity.

We start with a simple example. Consider the polynomial $f(x) = x^2$. We say that $f(x)$ has a double root (or a point of multiplicity 2) at $x = 0$, because in the factorisation of the polynomial, x has an exponent of 2. To motivate a more rigorous definition, consider the ideal $\langle x^2 \rangle$ in $K[x]$ and its corresponding variety $\boldsymbol{V}(I) = \{0\}$ in $\mathbb{A}K^2$. We see that the polynomial $g(x) = x$ lies in the ideal of the variety, $I(\boldsymbol{V}(I))$, but only a power (namely g^2) lies in the original ideal – this is the essence of Hilbert's

Nullstellensatz. Thus, we see that the polynomial generating the variety must have a higher multiplicity at $x = 0$ – the multiplicity being the power of g that lies in the original ideal. This clearly generalises to the polynomials $(x-\alpha)^n$, where $\alpha \in \mathbb{C}$, $n \in \mathbb{N}$.

What if we are faced with a more general polynomial $f(x) = (x-\alpha)^n g(x)$, where $g(\alpha) \neq 0$? In order to define the multiplicity of f at $x = \alpha$, we would need to "isolate" the term $(x-\alpha)$ from the polynomial. This **localisation** of the ring $K[x]$ at $x = \alpha$ can be achieved by the following definition:

Definition 3.1.1. Let R be a ring, $D \subset R \backslash \{0\}$ be multiplicatively closed in R. Then the localisation of R at D, written R_D, is the ring $R \times D/\sim$ under the equivalence relation

$$(a,b) \sim (c,d) \iff (ad-bc)h = 0 \text{ for some } h \in D.$$

We can think of an element (s,t) as the fraction $\frac{s}{t}$. The localisation of a ring at D is a generalisation of the well-known construction of the field of fractions, which uses the maximal ideal M of the ring.

To construct a definition of multiplicity of a root in an arbitrary polynomial, we use the set $D_\alpha = \{s(x) \in k[x] \mid s(\alpha) \neq 0\}$ and denote the corresponding local ring $K[x]_{D_\alpha}$ simply by R_α. Essentially, R_α is $K[x]$, but we are allowed to divide by polynomials not in the ideal $\langle x-\alpha \rangle$. Similarily, we denote the image of an ideal $I \subset K[x]$ in R_α by I_α.

Let us return now to the question of how to define the multplicity of $f(x) = (x-\alpha)^n g(x)$ at $x = \alpha$. If we consider the image $\overline{f}$ of f in R_α and use the fact that $g(\alpha) \neq 0$, we see that $\overline{f} \equiv (x-\alpha)^n$. Now, we may apply the same idea as above: Consider the local ideal $I_\alpha = \langle (x-\alpha)^n \rangle$ and its corresponding variety $\boldsymbol{V}(I_\alpha) = \{\alpha\}$. Then $(x-\alpha) \in I(\boldsymbol{V}(I_\alpha))$, but only $(x-\alpha)^n \in I_\alpha$. To capture this phenomenon, we may define the multiplicity of f at $x = \alpha$ to be

$$\begin{aligned} \dim_K \frac{R_\alpha}{\langle f \rangle_\alpha} &= \dim_K \frac{R_\alpha}{\langle (x-\alpha)^n \rangle_\alpha} \\ &= \dim_K \langle 1, x, \ldots, x^{n-1} \rangle = n. \end{aligned}$$

A generalisation to several variables is quite natural: suppose we are given an ideal $I = \langle f_1, \ldots, f_n \rangle$ and a point $P \in \boldsymbol{V}(I)$. First, we localise the ideal at P, obtaining

I_P. The intersection multiplicity is then simply $\dim_K \frac{R_P}{I_P}$.

Consider the following example: Take the ideal $I = \langle x^2(1-x), y\rangle$ in $\mathbb{Q}[x,y]$. Clearly, $\boldsymbol{V}(I) = \{(0,0),(1,0)\}$. If we localise at $P_1 = (0,0)$, we get the local ideal $I_{P_1} = \langle x^2, y\rangle$. It is easy to see that

$$\begin{aligned}\dim_K \frac{R_{P_1}}{\langle x^2(1-x), y\rangle_{P_1}} &= \dim_K \frac{R_{P_1}}{\langle x^2, y\rangle_{P_1}} \\ &= \dim_K \langle 1, x\rangle = 2.\end{aligned}$$

Localising at $P_2 = (1,0)$, on the other hand, we get the ideal $I_{P_2} = \langle 1-x, y\rangle$ with

$$\begin{aligned}\dim_K \frac{R_{P_2}}{\langle x^2(1-x), y\rangle_{P_2}} &= \dim_K \frac{R_{P_2}}{\langle 1-x, y\rangle_{P_2}} \\ &= \dim_K \langle 1\rangle = 1.\end{aligned}$$

Let us look at a slightly more complicated example: consider the curves

$$\begin{aligned}a(x,y) &= y^3 - x^2 \\ b(x,y) &= y^3 - x^2(1-x).\end{aligned} \tag{3.1}$$

Clearly, $(0,0) \in \boldsymbol{V}(a,b)$ over $\mathbb{AC}^2$, but what is the multiplicity of intersection here? If we look at the ideal $I = \langle y^2 - x^3, y^2 - x^2(1-x)\rangle$, we see that finding a basis for the localised ideal from this basis is not as straightforward as in the previous case. However, Gröbner Bases come to the rescue: If we compute the Gröbner Basis G with respect to $plex(x,y)$, we know that we will get an element $g_1(y) \in G$ in y only. Removing all factors except y^k for some $k \in \mathbb{N}$ in $g_1(y)$, we can then use this element to simplify the remaining elements of the Gröbner Basis further. In this case, $G = \{y^2(8y^2-1), y^2(2x-1), x^2 - 2y^2\}$. Localising this, we get $G_P = \{y^2, x^2 - 2y^2\}$, so

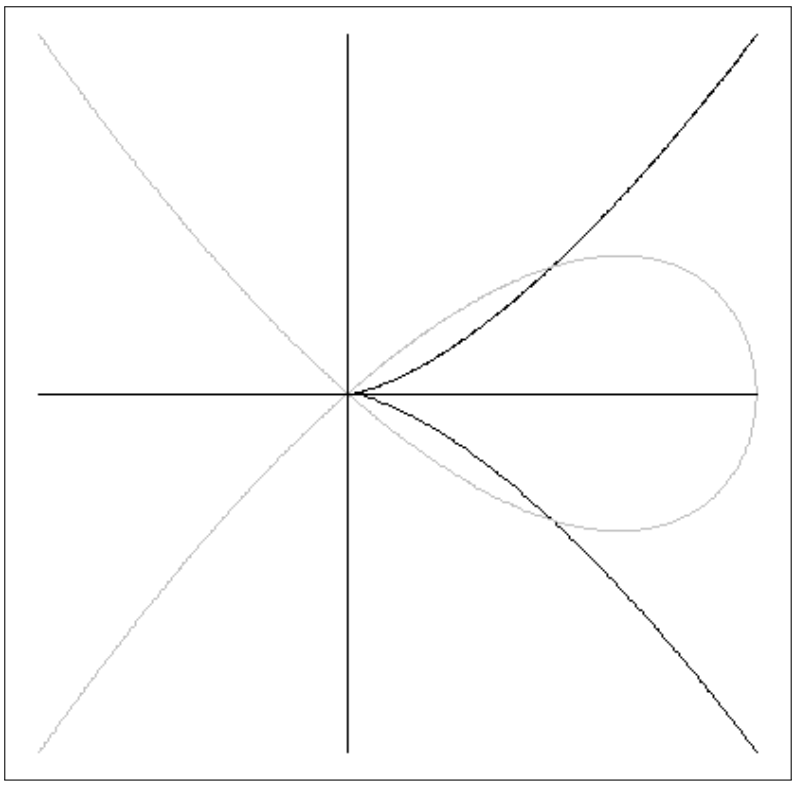

Figure 3.1: Affine versions of a (black) and b (grey) in (3.1)

that

$$\begin{aligned} I &= \langle y^2 - x^3, y^2 - x^2(1-x) \rangle \\ &= \langle y^2, x^2 - 2y^2 \rangle \\ &= \langle y^2, x^2 \rangle \end{aligned}$$

and the multiplicity here is $\dim_{\mathbb{Q}} \langle 1, x, y, xy \rangle = 4$.

We will repeat this definition of intersection multiplicity for two algebraic curves for reference:

Definition 3.1.2. Let f, g be algebraic curves and $P \in \mathbb{A}K^2$. We define the multiplicity of intersection of f and g at P by

$$i_P(f,g) = \dim_K \frac{R_P}{\langle f, g \rangle_P}$$

Note that the intersection multiplicity, as follows from the definition, is a purely local object. Thus, we do not need to define intersection multiplicity for projective

curves, as we can always localise to some affine chart defined at P and compute the intersection multiplicity of the corresponding affine curves at P. That the multiplicity obtained does not depend on the affine chart chosen is a consequence of the fact that any two affine charts $\mathbb{A}_1K^2$ and $\mathbb{A}_2K^2$ agree on their intersection in $\mathbb{P}K^2$. Thus, we will simply take $i_P(f,g)$ for projective curves f,g to mean the intersection multiplicity of suitable affine versions of f and g defined at P.

As we noted earlier, the multiplicity of intersection of f and g at a point $P = (\alpha,\beta,\gamma)$ may also be defined as the multiplicity of the root β of $\mathrm{Res}_x(f,g)$, provided the curves are in good position. We shall now show that this definition indeed agrees with the algebraic version in Definition 3.1.2.

Proposition 3.1.1. *Let $f,g \in K[x,y,z]$ be in good position with $\gcd(f,g) = 1$, $P = (\alpha,\beta,\gamma) \in \mathbb{P}K^2$ be a common point of f,g. Then $i_P(f,g)$ is the exponent of $y-\beta z$ of the factorisation of $\mathrm{Res}_x(f,g)$.*

Proof. First, note that we have $\langle \mathrm{Res}_x(f,g)\rangle \subset \langle f,g\rangle$ by Lemma 2.2.3, so that

$$\dim_K \frac{R_P}{\langle \mathrm{Res}_x(f,g)\rangle_P} \geq \dim_K \frac{R_P}{\langle f,g\rangle_P} = i_P(f,g). \tag{3.2}$$

That this first dimension is exactly the exponent of $y-\beta z$ in $\mathrm{Res}_x(f,g)$ simply follows from the fact that, localised at P, $\langle \mathrm{Res}_x(f,g)\rangle_P = \langle (y-\beta z)^k\rangle_P$.

Knowing this, suppose now that $k > i_P(f,g)$. Assuming Bézout's Theorem (which is completely independent of this argument), and summing over all $P_j \in \mathbb{P}K^2$ (and using (3.2)), we get that

$$\partial f \partial g = \partial \mathrm{Res}_x(f,g) = \sum_j k_j > \sum_{P_j} i_{P_j}(f,g) = \partial f \partial g,$$

which is clearly a contradiciton. Thus, $k = i_P(f,g)$. □

From the purely algebraic definition of intersection multiplicity, we can deduce a few basic properties of the multiplicity of intersection as in Definition 3.1.2.

Lemma 3.1.1. *Let $P \in \mathbb{A}K^2$ and $a,b,c \in K[x,y]$ with $\gcd(a,b) = \gcd(a,c) = 1$. Then*

(a) *If $a(P) \neq 0$ or $b(P) \neq 0$, then $i_P(a,b) = 0$*

(*b*) $i_P(a,b) = i_P(b,a)$

(*c*) $i_P(a,bc) = i_P(a,b) + i_P(a,c)$

(*d*) $i_P(a,b+ac) = i_P(a,b)$ *if* $\partial(ac) = \partial b$

(*e*) $i_P(a,b) \leq i_P(a,ma+nb), m,n \in K[x,y]$.

Proof. To prove (a), assume $a(P) \neq 0$, Then, for any $\frac{s}{t} \in R_P$, $\frac{s}{t} = \frac{as}{at} \in \langle a,b\rangle_P$, so that $i_P(a,b) = 0$. A similar argument applies if $b(P) \neq 0$.

The second and penultimate property are immediately obvious, since $\langle a,b\rangle_P = \langle b,a\rangle_P$ and $\langle a,b+ac\rangle_P = \langle a,b\rangle_P$.

For (c), we follow the proof from [21]. Define two maps

$$\psi : \frac{R_P}{\langle a,c\rangle_P} \to \frac{R_P}{\langle a,bc\rangle_P},\ \overline{z} \mapsto \overline{b'z}$$
$$\varphi : \frac{R_P}{\langle a,bc\rangle_P} \to \frac{R_P}{\langle a,b\rangle_P},\ \overline{z} \mapsto \overline{z},$$

where $\overline{z}$ denotes the residue of z in the corresponding quotient ring, and $b' = \frac{b}{w^k}$ where $k = \partial b$ and w is one of x,y,z, chosen such that $w \neq 0$ at P.

It is easy to check that ψ is a K-linear map. Further, if

$$\psi(\overline{z}) = \overline{0}$$

we get

$$b'z = sa + tbc,\ s,t \in R_P.$$

Upon clearing the least common denominator u of b,z,s,t, we get

$$bd = s^*a + t^*bc$$
$$s^*a = b(d - t^*c).$$

As $\gcd(a,b)=1$, $a \mid (d - t^* c)$, giving

$$d = af + t^* c,\ f \in K[x,y]$$
$$z = \frac{f}{u}a + \frac{t^*}{u}c$$

so that $\overline{z} = \overline{0}$ in $R_P / \langle a, c\rangle_P$, so ψ is injective.

Also, it is easy to check that φ is onto, so that the sequence

$$0 \longrightarrow \frac{R_P}{\langle a,c\rangle_P} \xrightarrow{\psi} \frac{R_P}{\langle a,bc\rangle_P} \xrightarrow{\varphi} \frac{R_P}{\langle a,b\rangle_P} \longrightarrow 0$$

is exact. By the rank-nullity theorem from linear algebra, this then implies that

$$\dim_K \frac{R_P}{\langle a,b\rangle_P} + \dim_K \frac{R_P}{\langle a,c\rangle_P} = \dim_K \frac{R_P}{\langle a,bc\rangle_P}.$$

To prove (d), note that we have a containment of ideals $\langle a, ma+nb\rangle \subset \langle a,b\rangle$. Thus,

$$i_P(a,b) = \dim_K \frac{R_P}{\langle a,b\rangle_P} \leq \dim_K \frac{R_P}{\langle a, ma+nb\rangle_P} = i_P(a, ma+nb). \qquad \square$$

Using this definition and its properties, we define the notion of the intersection cycle $a \cdot b$ of two algebraic curves:

Definition 3.1.3. Let $a, b \in K[x,y,z]$ be projective algebraic curves. We define the intersection cycle $a \cdot b$ of a and b to be the divisor

$$a \cdot b = \sum_{P \in \mathbb{P}K^2} i_P(a,b)P.$$

It is easily verified that the properties of intersection multiplicity carry over to intersection cycles. For reference, we state this as a corollary.

Corollary 3.1.1. *Let $a, b, c \in K[x,y,z]$. We have*

1. $a \cdot b = b \cdot a$
2. $a \cdot (bc) = a \cdot b + a \cdot c$

3. $a \cdot (b + ac) = a \cdot b$ *if* $\partial ac = \partial b$.

This definition, together with the Euclidean algorithm for polynomials, forms the basis for our intersection algorithm for algebraic curves, outlined in the next section.

3.2 An intersection algorithm based on the Euclidean Algorithm

In this section, we will use the properties of the intersection cycle outlined in the previous section to derive a method for expressing the intersection cycle of algebraic curves a, b over $\mathbb{P}K^2$ in terms of intersection cycles of curves with products of lines. We will then show how to solve this easier problem and use the solution to build up the intersection cycle of the original curves.

3.2.1 Reducing the general intersection problem using the division algorithm

We start with a given pair of algebraic curves $a, b \in K[x, y, z]$ and no common component. Considering these curves as polynomials in $K[y, z][x]$, we may use the polynomial division algorithm on the variable x to write

$$da = bq + r,$$

where we have cleared denominators $d \in K[y, z]$ out of the usual form of the division algorithm to get $q, r \in K[x, y, z]$ with $\partial_x r < \partial_x b$.

Suppose now that $g = \gcd(b, r)$. As $\gcd(a, b) = 1$, it is clear that also $g = \gcd(b, d)$, so we divide through by g to get

$$d'a = qb' + r', \tag{3.3}$$

where now $\gcd(b', r') = \gcd(b', d') = 1$. Taking now the intersection cycle of both

sides of this with b' and using Corollary 3.1.1, we get

$$\begin{aligned} b' \cdot (d' a) &= b' \cdot (q b' + r') \\ b' \cdot d' + b' \cdot a &= b' \cdot r' \\ a \cdot b' &= b' \cdot r' - b' \cdot d'. \end{aligned}$$

Since $b = b'g$, we see that then

$$\begin{aligned} a \cdot b &= a \cdot (b'g) \\ &= b' \cdot r' - b' \cdot d' + a \cdot g. \end{aligned} \tag{3.4}$$

Note that that the right-hand side of (3.4) consists of intersection cycles of curves of lower x-degree and intersection cycles of curves of the form $c_1 \cdot c_2$ with $\partial_x c_2 = 0$, as $\partial_x g = 0$, (recall that $g \mid d \in K[y,z]$).

Let $p_{-1} = a, p_0 = b, d_0 = d', p_1 = r'$. In the following, as above, a $'$ indicates that the gcd has been removed from the polynomials. Repeatedly applying (3.3), we get

$$\begin{aligned} d_0 p_{-1} &= q_0 p_0' + p_1 \\ d_1 p_0' &= q_1 p_1' + p_2 \\ &\vdots \\ d_{n-1} p_{n-2}' &= q_{n-1} p_{n-1}' + p_n \end{aligned} \tag{3.5}$$

where $\partial_x p_{n-1} > 0$ and $\partial_x p_n = 0$. The corresponding expressions for the curves will read

$$\begin{aligned} p_{-1} \cdot p_0 &= p_0' \cdot p_1 - p_0' \cdot d_0 + p_{-1} \cdot g_0 \\ p_0' \cdot p_1 &= p_1' \cdot p_2 - p_1' \cdot d_1 + p_0' \cdot g_1 \\ &\vdots \\ p_{n-2}' \cdot p_{n-1} &= p_{n-1}' \cdot p_n - p_{n-1}' \cdot d_{n-1} + p_{n-2}' \cdot g_{n-1}. \end{aligned} \tag{3.6}$$

Collecting these expressions together, we have

$$a \cdot b = p_n \cdot p'_{n-1} + \sum_{i=1}^{n-1} \left(p'_{i-1} \cdot g_i - p'_i \cdot d_i \right) + p_{-1} \cdot g_0 - p'_0 \cdot d_0. \tag{3.7}$$

As all $d_i, g_i \in K[y,z]$, we have now reduced the problem of finding the intersection cycle $a \cdot b$ to the problem of finding intersection cycles $c_1 \cdot c_2$, where $\partial_x c_2 = 0$.

3.2.2 Intersecting a curve with a product of lines

In the previous section, we showed how to reduce the general intersection problem to the problem of intersecting curves a, b with $a \in K[x,y,z], b \in K[y,z]$. For this section, assume that K is algebraically closed.

As $b(y,z)$ is homogeneous, we may write it as

$$b(y,z) = \lambda z^k \prod_{i=1}^{m} (y - \beta_i z)^{k_i}.$$

Using the properties of intersection cycles, we get

$$\begin{aligned} a \cdot b &= a \cdot \left(z^k \prod_{i=1}^{m} (y - \beta_i z)^{k_i} \right) \\ &= k(a \cdot z) + \sum_{i=1}^{m} k_i \left(a \cdot (y - \beta_i z) \right). \end{aligned}$$

Consider the expansion of $a(x,y,z)$ in two different ways:

$$a(x,y,z) = \begin{cases} \sum_{j=0}^{\partial_z a} a_j(x,y) z^j \\ \sum_{j=0}^{\partial_y a} \widetilde{a_j}(x,z)(y - \beta_i z)^j, \ 1 \le i \le m \end{cases}$$

Using these expressions, together with Corollary 3.1.1(c), we get

$$a \cdot z = a_0 \cdot z$$

$$a \cdot (y - \beta_i z) = \widetilde{a_0} \cdot (y - \beta_i z)$$

As the resulting polynomials $a_0(x,y) = \mu \prod_s l_s^{m_s}$ and $\widetilde{a_0}(x,z;\beta_i) = \eta \prod_t \widetilde{l_t}^{n_t}$ are products

of lines themselves, we have

$$a \cdot b = k \sum_s m_s (l_s \cdot z) + \sum_i k_i \left(\sum_t n_t \left(\widetilde{l}_t \cdot (y - \beta_i z) \right) \right), \tag{3.8}$$

written as a sum of intersections of lines, which can be computed using (1.3).

3.2.3 An example

Let us consider an example. Let $a, b \in \mathbb{Q}[x, y, z]$ be given by

$$a(x, y, z) = x^3 y^2 - x z^4 + y^2 z^3$$
$$b(x, y, z) = xy + xz + yz,$$

as in (2.4) in the previous section.

Using the Euclidean algorithm, we write $d\,a = bq + r$ with

$$r(y, z) = yz^4(3y^3 + 4y^2 z + 3z^2 y + z^3)$$
$$d(y, z) = (y + z)^3$$

We have $\gcd(b, r) = \gcd(b, d) = 1$, which simplifies the expression for $a \cdot b$ down to

$$a \cdot b = b \cdot r - b \cdot d.$$

One easily finds that

$$b \cdot d = 6 \cdot (1, 0, 0).$$

simply by substituting $y = -z$ into $b(x, y, z)$ and solving the resulting equation for x/z. To compute $b \cdot r$, we intersect each factor of r with b, in turn. We get:

$$b(x, y, z) \cdot y = (1, 0, 0) + (0, 0, 1)$$
$$b(x, y, z) \cdot z^4 = 4 \cdot (1, 0, 0) + 4 \cdot (0, 1, 0)$$
$$b(x, y, z) \cdot p(y, z) = \sum_\alpha \left(-\frac{\alpha}{1 + \alpha}, \alpha, 1 \right) + 3 \cdot (1, 0, 0),$$

where α is a root of $p(y,1)$ with $p(y,z) = 3y^3 + 4y^2z + 3z^2y + z^3$. Thus, we get

$$\begin{aligned} a \cdot b &= b \cdot r - b \cdot d \\ &= 2 \cdot (1,0,0) + 4 \cdot (0,1,0) + (0,0,1) \\ &\quad + \sum_{\alpha} \left(-\frac{\alpha}{1+\alpha}, \alpha, 1 \right), \end{aligned}$$

where the sum is taken over the conjugates of α over $\mathbb{Q}$.

Note that the multiplicities indeed add up to $2+4+1+3 = 10$ (remembering that there are three distinct values for α), as Bézout's theorem predicts.

3.3 Bézout's Theorem

The observation from the previous example is not a coincidence: the intersection algorithm can be used to give a basic recursive proof of Bézout's Theorem:

Theorem 3.3.1. *Let K be algebraically closed and suppose a, b are projective curves over $\mathbb{P}K^2$. Then*

$$\sum_{P \in \mathbb{P}K^2} i_P(a,b) = \partial a \partial b.$$

Proof. We proceed by induction on the x-degree of b. For the base case, let $b \in K[y,z]$ only. Using the notation from Section 3.2.2, we see from (3.8) that

$$\begin{aligned} \sum_{P \in \mathbb{P}K^2} i_P(a,b) &= k \sum_s m_s + \sum_i k_i \left(\sum_t n_t \right) \\ &= k\partial a + \sum_i k_i \partial a \\ &= \partial a \partial b, \end{aligned}$$

as $\partial a = \partial a_0 = \partial \widetilde{a_0}$ by homogeneity and we have used the fact that $k + \sum_i k_i = \partial b$.

Suppose now that we have the result for all pairs of curves a, b with $\partial_x b < n \in \mathbb{N}$

and suppose we are given a, b with $\partial_x b = n$. From (3.4), we have

$$\begin{aligned}\sum_{P \in \mathbb{P}K^2} i_P(a,b) &= \partial b'(\partial r' - \partial d') + \partial a \partial g \\ &= \partial b' \partial a + \partial a \partial g \\ &= \partial a \partial b,\end{aligned}$$

as $\partial r' = \partial(d'a) = \partial d' + \partial a$ by homogeneity and $\partial b = \partial b' g = \partial b' + \partial g$. □

Chapter 4

Bézout's Theorem over General Fields

Clearly, Bézout's Theorem cannot hold if the underlying field is not algebraically closed, as it does not even apply in the univariate case – the intersection of a polynomial in $\mathbb{Q}[x]$ with the x-axis $y = 0$, for example. One can, however, start with a general field K and attempt to find the smallest extension L/K such that Bézout's Theorem holds for a given pair of curves. The purpose of this section is to give a constructive method for finding this extension, using the algorithm introduced in the previous section.

As the recursive steps in the algorithm do not involve any explicit computations of intersection points, we only need to consider the case of intersecting curves $a \in K[x, y, z], b \in K[y, z]$, as outlined in the proof of Bézout's Theorem. The general case then follows from applying the methods from the previous chapter.

4.1 Constructing the smallest extension over which Bézout's Theorem holds

Recall that, in the case $\partial_x b = 0$, the intersection points were obtained by first factorising $b(y, z)$ into linear factors and then in turn intersecting these linear factors with a. The polynomial resulting from this substitution was then factorised again, its roots giving the remaining coordinates of the point. Now, as we are dealing with a not algebraically closed field, the roots of $b(y, z)$ will lie in an extension L_1/K. The resulting polynomials $a_0, \widetilde{a_0}$ will then have roots in an extension L_2/L_1. Thus,

intersection points will be of the form

$$P = \begin{cases} (\alpha, \beta, 1) & \text{if} \quad l = y - \beta z \\ (\alpha, 1, 0) & \text{if} \quad l = z \end{cases},$$

where l represents the factor of $b(y,z)$ corresponding to P. Here, α in the first case is defined over an extension of K containing β. The smallest extension L_2/K such that $P \in \mathbb{P}L_2^2$ is then $L_2 = K(\alpha) \supset K(\beta)$, and consequently, the smallest extension over which Bézout's Theorem holds is the extension $K(\gamma)$, generated by the element

$$\gamma = \sum_i c_i \alpha_i,$$

the sum taken over all common points P_i of the curves. Here, the $c_i \in K$ are chosen to guarantee $\prod_i \partial\alpha_i$ distinct values of γ.[1]

If we are faced with two arbitrary curves, we know that its intersection cycle may be expressed in the form (3.7). The smallest extension L/K is then the extension obtained by combining the algebraic elements in the coordinates of all points in these intersection cycles – after having combined common points across different cycles. This particular step may cause problems, however, as the following section shows.

4.2 A problematic example

While the calculation of the extension is straightforward if one of the polynomials is constant in x, the recursive definition of the general intersection cycle $a \cdot b$ leads to problems, as the following example shows:

Let

$$a(x,y,z) = x^4$$
$$b(x,y,z) = (y^4 + z^4)x^4 + (xz^2 - yz^2 + y^3 - z^3)(x^2 - 2xz - z^2)z^3.$$

[1] This guarantees that $\alpha_i \in K(\sum_i c_i \alpha_{i,j_i})$, for any choice of conjugates α_{i,j_i} of α_i. In the case $\alpha_1 = \sqrt{2}+\sqrt{5}, \alpha_2 = \sqrt{2}+\sqrt{3}$, there are two choices of conjugates of the elements that result in a value of $\gamma = \sqrt{3}+\sqrt{5}$, but $\alpha_1, \alpha_2 \notin K(\sqrt{3}+\sqrt{5})$.

We start by applying the Euclidean algorithm to write $da = bq + r$ with

$$d(y,z) = y^4 + z^4$$
$$r(x,y,z) = -z^3(x^2 - 2xz - z^2)(xz^2 - yz^2 + y^3 - z^3).$$

Using properties of the intersection cycle from Corollary 3.1.1, we see that $b \cdot r = b^* \cdot r$ with $b^*(x,y,z) = x^4 d(y,z)$ and that $b \cdot d = r \cdot d$. Thus, the intersection cycle $b \cdot r$ contains (as part of the formal sum) the intersection cycle $d \cdot s_2$, with

$$s_2(x,y,z) = xz^2 - yz^2 + y^3 - z^3.$$

This intersection cycle in turn contains the point $P = (1+\sqrt{2}, \frac{1}{\sqrt{2}}(1+i), 1)$, expressed as $(\beta_1 - \beta_1^3 + 1, \beta_1, 1)$, where $\beta_1 = \frac{1}{\sqrt{2}}(1+i)$ is a root of $y^4 + 1$.

The intersection cycle of b and d, on the other hand, contains the intersection cycle $d \cdot t$, where $t(x,z) = x^2 - 2xz - z^2$. This cycle contains the point $P' = (1 + \sqrt{2}, \frac{1}{\sqrt{2}}(1+i), 1)$, this time expressed as $P' = (\alpha_1, \beta_1, 1)$, where $\alpha_1 = 1 + \sqrt{2}$, the first root of $x^2 - 2x - 1$, and β_1 is as above. While it is clear that P and P' represent the same point, the point will appear in different representations in the two cycles. To combine points across representations in $a \cdot b$, we thus need to find a way of comparing points expressed in terms of different extensions over K.

4.3 Comparing points across representations

4.3.1 Algebraic n-tuples

Instead of considering points, we will be working with n-tuples of algebraic elements over K – we will refer to them as *algebraic n-tuples*. We want to be able to determine if two algebraic n-tuples are equivalent. The natural way to do this is through the use of automorphisms:

Definition 4.3.1. Let $n \in \mathbb{N}$, $\boldsymbol{\alpha} = (\alpha_1, \ldots \alpha_n)$, $\boldsymbol{\beta} = (\beta_1, \ldots \beta_n)$ be algebraic n-tuples over a field K. We define a relation $\simeq$ on the set of algebraic n-tuples by $\boldsymbol{\alpha} \simeq \boldsymbol{\beta}$ if there exists an automorphism

$\sigma \in \mathrm{Gal}(K(\alpha_1,\dots\alpha_n,\beta_1,\dots\beta_n)/K)$ such that

$$\sigma\boldsymbol{\alpha} = (\sigma\alpha_1,\dots\sigma\alpha_n) = (\beta_1,\dots,\beta_n).$$

Two algebraic n-tuples equivalent under this relation are the same n-tuple with coordinates expressed in terms of different algebraic extensions of K. We will call the equivalence class $[\boldsymbol{\alpha}]$ the *Galois orbit* of $\boldsymbol{\alpha}$.

It is clear that P and P' from the previous section are equivalent using this definition, as $\mathbb{Q}(1+\sqrt{2},\beta_1) = \mathbb{Q}(\beta_1)$. If the n-tuples represent points on an algebraic curve with coefficients in K, it is further clear that the entire Galois orbit lies on the curve. Further, the multiplicity of a point of intersection of two curves is clearly an invariant of the Galois orbit.

Given this equivalence relation, it is convenient to have a way of determining when two Galois orbits are the same. As we are dealing with algebraic elements, a natural way is to represent the Galois orbits using the minimal polynomials of the algebraic elements.

As $[K(\alpha_1,\dots\alpha_n):K]$ is finite and $K(\alpha_1,\dots\alpha_n)$ only has finitely many intermediate subfields over K, the Primitive Element Theorem (see [12] for example) tells us that there exists a $\gamma \in K(\alpha_1,\dots,\alpha_n)$ such that $K(\alpha_1,\dots\alpha_n) = K(\gamma)$. Now, let $N = [K(\gamma):K]$ and let $c_0, c_1, \dots c_{N-1} \in K$ be unknowns. Fix some α_i and consider now the equation

$$c_0 + c_1\gamma + \dots + c_{N-1}\gamma^{N-1} = \alpha_i$$

By applying automorphisms in $\mathrm{Gal}(K(\gamma)/K)$, we get a system of at most N equations, expressing the conjugates $\alpha_{i,j}$, $j = 1,\dots,d_i (= \partial\alpha_i)$ of α_i in terms of the polynomial $p(x) = \sum_{i=0}^{N-1} c_i x^i$ evaluated at conjugates of γ. This can be written as

$$\boldsymbol{\Gamma}\boldsymbol{c} = \boldsymbol{\alpha}$$

Here, $\boldsymbol{\Gamma}$ is the Vandermonde Matrix with entries $\boldsymbol{\Gamma}_{i,j} = \gamma_i^j$, where γ_i denotes the i^{th} conjugate of γ, $\boldsymbol{c} = (c_0,\dots c_n)$, and $\boldsymbol{\alpha} = (\alpha_{i,1},\dots\alpha_{i,d_i},\dots\alpha_{i,1},\dots\alpha_{i,d_i})$ contains the conjugates of α_i repeated $[K(\gamma):K(\alpha_i)]$ times.

Upon inverting $\boldsymbol{\Gamma}$ (see Appendix A), we get a polynomial expression $p_i(\gamma) = \alpha_i$,

$p_i(x) \in K[x]$. Thus, we can represent $(\alpha_1, \dots \alpha_n)$, together with all conjugate n-tuples, as

$$[(p_1(x), \dots, p_n(x)), q_\gamma(x)]$$

where $q_\gamma(x) \in K[x]$ is the minimal polynomial of γ over K. We call this the *polynomial representation* of the Galois orbit of the algebraic n-tuple $(\alpha_1, \dots \alpha_n)$. In the case of P and P' in the example above, we get polynomial representations

$$\begin{aligned} [P] &= \left[(-x^3 + x + 1, x, 1), x^4 + 1\right] \\ \left[P'\right]_1 &= \left[\left(\frac{1}{5} + \frac{2}{3}x + \frac{1}{5}x^2 - \frac{1}{15}x^3, -\frac{1}{5} + \frac{1}{3}x - \frac{1}{5}x^2 + \frac{1}{15}x^3, 1\right),\right. \\ &\quad \left. x^4 - 4x^3 - 2x^2 + 12x + 18\right]. \end{aligned} \tag{4.1}$$

$[P']$ in this case actually splits into two disjoint orbits $[P']_1, [P']_2$. The orbit $[P']_1$, given above, represents the 4 points that also occur in the orbit $[P]$. The remaining points lie in the orbit

$$[P']_2 = [(1 - 2x + 3x^2 - x^3, -1 + 3x - 3x^2 + x^3, 1), x^4 - 4x^3 + 6x^2 - 4x + 2].$$

It is far from obvious that the Galois orbits in (4.1) are indeed the same. The following theorem will give us a way of proving this.

Theorem 4.3.1. *Let* $[\boldsymbol{a}] = [(p_1(x), \dots, p_n(x)), q_\theta(x)], [\boldsymbol{b}] = [(r_1(x), \dots, r_n(x)), q_\delta(x)]$ *be polynomial representations of Galois orbits. Further, let*

$$H(t_1, \dots t_n) = \mathrm{Res}_y\left(\mathrm{Res}_x\left(\sum_{j=1}^{n} t_j(p_j(x) - r_j(y)), q_\theta(x)\right), q_\delta(y)\right).$$

Then $[\boldsymbol{a}] = [\boldsymbol{b}]$ *if and only if* $H(t_1, \dots t_n) \equiv 0$.

Proof. Denote by θ_j any conjugate of θ and by δ_k a conjugate of δ. Then for $[\boldsymbol{a}] = [\boldsymbol{b}]$, we need, for any $i = 1, \dots, n$, some j, k with $p_i(\theta_j) = r_i(\delta_k)$. Let $t_i, i = 1, \dots, n$ be

arbitrary in L. Then this can be rewritten as

$$\sum_{i=1}^{n} t_i(p_i(\theta_j) - r_i(\delta_k)) = 0 \iff \mathrm{Res}_x\left(\sum_{i=1}^{n} t_i(p_i(x) - r_i(\delta_k)), q_\theta(x)\right) = 0$$
$$\iff H(t_1, \ldots, t_n) \equiv 0. \qquad \square$$

Using this, it can be easily checked that $[P] = [P']_1$.

Chapter 5

Computational Implementation

By its recursive nature, the algorithm outlined in Chapter 3 lends itself well for implementation in a computing package such as Maple. When implementing a version over $\mathbb{Q}$, the theory from Chapter 4 can be used to compare points across representations explicitly.

A highly documented version of a Maple implementation can be found at [31].

Part II

Integer polynomials with all roots in a given real interval and the integer (monic) transfinite diameter

Chapter 6

Introduction

6.1 Polynomials with all roots in an interval and the transfinite diameter

Given a polynomial $p(x) = a_d x^d + \ldots + a_0 = a_d \prod_{i=1}^{d}(x - \alpha_i)$, it is a natural question to try to find the zeros of $p(x)$. In the case of real zeros, this can be done using Newton's Method, for example. One can also turn this question around and ask, given an interval I on the real line, to describe all polynomials having their roots in the interval. Of course, this is only interesting for polynomials with integer coefficients, as otherwise an arbitrary set of reals $\{\alpha_1, \ldots, \alpha_d\} \subset I$ yields the polynomial $\prod_{i=1}^{d}(x-\alpha_i)$ with real coefficients and all roots in I.

For a closed and bounded interval $I \subset \mathbb{R}$, let us define

$$\mathscr{L}_I(a,d) = \left\{ p(x) = a\prod_{i=1}^{d}(x-\alpha_i) \in \mathbb{Z}_d[x] : \alpha_i \in I, 1 \le i \le d \right\}$$

where $I \subset \mathbb{R}$ is a fixed real interval, and set $\mathscr{L}_I(a) = \bigcup_{d=1}^{\infty} \mathscr{L}_I(a,d)$. In [14], Fekete defined the so-called *transfinite diameter* $t(I)$ of an interval and showed that if, for some fixed $a \in \mathbb{N}$, $\mathscr{L}_I(a)$ is infinite, then $t(I) \ge 1$.

Later, Robinson [39] proved a partial converse of Fekete's first result, showing that real intervals I with $t(I) > 1$ have $|\mathscr{L}_I(1)| = \infty$. His result is easily generalised to algebraic numbers whose minimal polynomials have a fixed odd leading coefficient $a > 1$, as is shown in section 7.1.2.

As we will see later, for real intervals, $t(I) = \frac{|I|}{4}$, so that all of Fekete's results can be rephrased for intervals in terms of the length of the interval: for $a \in \mathbb{N}$, $\mathscr{L}_I(a)$ is finite when $|I| < 4$ and infinite when $|I| > 4$. The case $|I| = 4$ is, still today, unsolved, except for intervals of the form $I = [a, a+4]$, $a \in \mathbb{Z}$.

To retrace Fekete's steps, let us first turn to a different problem. Consider a compact set $E \subset \mathbb{C}$ and let $n \in \mathbb{N}$. Using the usual norm, one may try to find

$$\Delta_n(E) = \max_{z_1,\ldots,z_n \in E} \prod_{\substack{1 \le i,j \le n \\ i \ne j}} |z_i - z_j|,$$

where the maximum is taken over all n-element subset of E. The extremal points $z_1, \ldots, z_n$ are then called the n^{th} *Fekete points* of E and $\Delta_n(E)$ the n^{th} *Fekete constant*. Taking the $n(n-1)$-th root and letting $n \to \infty$, we get

$$\Delta(E) = \lim_{n\to\infty} \Delta_n(E)^{\frac{1}{n(n-1)}},$$

the so-called *transfinite diameter* of E.

One may now wonder about the connection between this particular problem and the above problem of finding all polynomials with integer coefficients and roots in a given interval. Consider the sets $\mathbb{C}_n^*[z]$ and $\mathbb{C}_n^*(E)$ of monic polynomials of degree n with complex coefficients (and all roots in the compact set $E \subset \mathbb{C}$). Let $\|p\|_E = \sup_{z\in E} |p(z)|$ denote the supremum norm of the polynomial $p(z)$ on E, and consider the two quantities

$$\mu_n(E) = \inf_{p \in \mathbb{C}_n^*[z]} \|p\|_E$$
$$\widetilde{\mu}_n(E) = \inf_{p \in \mathbb{C}_n^*(E)} \|p\|_E,$$

and then take the limit of the n^{th} root of these so-called n^{th} *Chebyshev constants*, to get

$$\mu(E) = \lim_{n\to\infty} \mu_n(E)^{\frac{1}{n}}$$
$$\widetilde{\mu}(E) = \lim_{n\to\infty} \widetilde{\mu}_n(E)^{\frac{1}{n}}.$$

One can show (as is done in the next section) that $\mu(E) = \widetilde{\mu}(E) = \Delta(E)$, so that the restriction on the location of the roots in $\widetilde{\mu}(E)$ is actually not necessary. In light of this, we will denote all these quantities by $t(E)$, the transfinite diameter, or Chebyshev constant, of the set E. For consistency, define $t_n(E) = \mu_n(E)$.

If $E = I = [-1,1] \subset \mathbb{R}$, $n \in \mathbb{N}$, the n^{th} extremal polynomial can be shown to be the Chebyshev polynomial

$$T_n(x) = \cos(n \arccos x) \tag{6.1}$$

with

$$t_n(I) = 2^{1-n} \|T_n\|_I = 2^{1-n}.$$

The Chebyshev constant of $I = [-1,1]$ is therefore the limit of the n^{th} root of this expression,

$$t(I) = \lim_{n\to\infty} 2^{\frac{1-n}{n}} = \tfrac{1}{2}.$$

This is easily generalised to an arbitrary closed interval $[a,b]$ of finite length $b-a>0$ on the real line, where the n^{th} extremal polynomial for the Chebyshev constant is simply

$$\widetilde{T_n}(x) = 2\left(\frac{b-a}{4}\right)^n T_n\left(\frac{2x-a-b}{b-a}\right) \tag{6.2}$$

giving a Chebyshev constant of

$$t([a,b]) = \frac{b-a}{4}.$$

Thus, the Chebyshev polynomials solve the problem of determining the Chebyshev constant for all real intervals. The problem can be made much more challenging by putting an additional requirement on the polynomials involved. If we define

$$\mathbb{Z}_n[x] = \left\{p_n(x) = a_n x^n + \ldots + a_0 : a_i \in \mathbb{Z}, 1 \le i \le n, a_n \neq 0\right\}$$

to be the set of integer polynomials of degree n, one can define a quantity similar to

the transfinite diameter by

$$t_{\mathbb{Z}}(I) = \lim_{n\to\infty} \inf_{0\neq p_n\in\mathbb{Z}_n[x]} \|p_n\|_I^{\frac{1}{n}},$$

the so-called *integer transfinite diameter*, or *integer Chebyshev constant*. Quite contrary to the results for the ordinary transfinite diameter, there is not a single real interval of length up to 4 (aside from single points), for which the integer transfinite diameter is known. Its determination is therefore a non-trivial problem.

It is known (see [22]) that for $|I| \geq 4$, $t_{\mathbb{Z}}(I) = t(I) = \frac{|I|}{4}$. Thus, we only need to consider intervals of length less than 4 throughout.

The integer transfinite diameter has received a lot of attention in the literature, but its actual value remains unknown for any interval of nonzero length less than 4. A theoretically interesting result in the area is an argument by Gelfond and Schnirelman (see [15]), showing that, if $t_{\mathbb{Z}}([0,1]) = \frac{1}{e}$ holds, a simple proof of the prime number theorem follows. Unfortunately, this is known not to be the actual value of $t_{\mathbb{Z}}([0,1])$.

There is a classical theorem (see [35], for example), stating that polynomials in $\mathbb{Z}_n(I)$ (with integer coefficients and all roots in the given interval I), and of sufficiently small normalised leading coefficient, must be factors of the Integer Chebyshev polynomials. Further, as is shown in [27], if infinitely many such polynomials exist, the integer transfinite diameter takes on the form

$$t_{\mathbb{Z}}(I) = \inf_k a_{d_k}^{-1/d_k},$$

where the infinimum is taken over all $q_k(x) = d_{d_k}x^{d_k} + \ldots + a_0 \in \mathbb{Z}_{d_k}(I)$ with $a_d > 1$ and $a_{d_k}^{1/d_k} < t_{\mathbb{Z}}(I)^{-1}$.

In the definition of the transfinite diameter, one can also restrict the polynomials further: if we take the infimum over monic polynomials in $\mathbb{Z}_n[x]$ only, we get the so-called *monic integer transfinite diameter* $t_M(I)$. In this case, if $q(x) = a_d x^d + \ldots + a_0 \in \mathbb{Z}_n(I)$ with $a_d > 1$, then $a_d^{-1/d} \leq t_M(I)$. This allows explicit computation of the monic integer transfinite diameter in a number of cases.

From this, it is clear that polynomials with integer coefficients and all roots in the interval I in question play a central role in the theory of the (monic) integer

transfinite diameter of I. Let $I = [a,b]$ be a closed real interval with $0 < |b-a| < 4$. We define

$$\mathscr{S}_I = \left\{ a_d^{1/d} : a_d x^d + \ldots + a_0 \in \mathbb{Z}_d(I), a_d > 1 \right\}$$

and call this the *spectrum* of I. In the following chapters, we will analyse this spectrum, showing, among other things, that

1. $\mathscr{S}_{[0,1]}$ is dense in (l,∞), where $l \approx 2.3768$. We then generalise this result to a larger class of intervals with rational endpoints.

2. $\mathscr{S}_{[0,1]}$ has only 6 distinct isolated points in $[1, 2.3647]$.

3. We will also analyse the relationship between $\inf \mathscr{S}_I$ and $t_M(I)$. We will show that this relationship does not always lead to a tight best possible lower bound on the monic integer transfinite diameter.

Note also that the gap between 2.3647 and 2.3768 cannot be closed using the computational methods outlined in the following chapters: Pritsker showed in [38] that the integer transfinite diameter is attained by an infinite product of distinct polynomials, so no search for a finite list of factors can produce the actual value of $t_{\mathbb{Z}}(I)$.

6.2 Proofs

We will provide proofs of two essential theorems in the introduction here. First, we show that, for a compact set $E \subset \mathbb{C}$, the Fekete constant $\Delta(E)$ is equivalent to the transfinite diameter $\mu(E)$. These proofs are sketched in [8], and we are merely filling in the details here.

We begin with a lemma:

Lemma 6.2.1. *Let $E \subset \mathbb{C}$ be compact. Then the sequence $\left\{ \Delta_n(E)^{\frac{1}{n(n-1)}} \right\}_{n=1}^{\infty}$ converges.*

Proof. We start by letting $q_n(x) = \prod_{i=1}^{n}(z - z_i)$, where $z_1, z_2, \ldots, z_n$ are the n^{th} Fekete points. Set

$$m_n = \min_{i=1,\ldots,n} |q_n'(z_i)|,$$

where $q_n'(z)$ denotes the derivative of $q_n(z)$.

Fixing $k \in \{1,\dots,n+1\}$, we may write

$$\begin{aligned}\Delta_{n+1}(E) &= \prod_{\substack{1\le i,j\le n+1\\ i\neq k, j\neq k, i\neq j}} |z_i - z_j| \prod_{\substack{1\le i\le n+1\\ i\neq k}} |z_k - z_i|^2 \\ &\le \Delta_n(E) \prod_{\substack{1\le i\le n+1\\ i\neq k}} |z_k - z_i|^2.\end{aligned}$$

Note that $q_n'(z_k) = \prod_{i\neq k} |z_k - z_i|$. Thus, by taking the minimum over all $i \in \{1,\dots,n+1\}$ in the above inequality, we get

$$\Delta_{n+1}(E) \le \Delta_n(E) m_{n+1}^2. \tag{6.3}$$

Also, we note that

$$\begin{aligned}m_{n+1} &= \min_{i=1,\dots,n+1} \prod_{i\neq j} |z_i - z_j|^{n+1} \\ &\le \prod_{1\le i\le n+1} \prod_{i\neq j} |z_i - z_j| \\ &\le \Delta_{n+1}(E).\end{aligned} \tag{6.4}$$

Taking (6.3) and (6.4) together, we obtain

$$\begin{aligned}\left(\frac{\Delta_{n+1}(E)}{\Delta_n(E)}\right)^{n-1} &\le \left(\frac{\Delta_n(E)}{\Delta_{n+1}(E)}\right)^2 \left(\frac{\Delta_{n+1}(E)}{\Delta_n(E)}\right)^{n+1} \\ &\le \Delta_n(E)^2\end{aligned}$$

so that

$$\Delta_{n+1}(E)^{\frac{1}{(n+1)n}} \le \Delta_n(E)^{\frac{1}{n(n-1)}}.$$

Since $\Delta_n(E)$ is always non-negative (and thus bounded below), this guarantees the existence of

$$\Delta(E) = \lim_{n\to\infty} \Delta_n(E)^{\frac{1}{n(n-1)}}$$

by the monotone convergence theorem. □

Another Lemma shows the corresponding result for the transfinite diameter. The proof follows an argument from Pólya and Szegö in [36].

Lemma 6.2.2. *Let $E \subset \mathbb{C}$ be compact. Then the sequence $\left\{\mu_n(E)^{\frac{1}{n}}\right\}_{n=1}^{\infty}$ converges to its infimum.*

Proof. First, note that, for $n, m \in \mathbb{N}$,

$$\begin{aligned}\mu_{n+m}(E) &= \inf_{p\in\mathbb{C}_{n+m}[x]} \|p\|_E \\ &= \inf_{q\in\mathbb{C}_n[x], r\in\mathbb{C}_m[x]} \|qr\|_E \\ &\leq \inf_{q\in\mathbb{C}_n[x], r\in\mathbb{C}_m[x]} \|q\|_E \|r\|_E \\ &\leq \mu_n(E)\mu_m(E).\end{aligned}$$

Let $a_n = \log \mu_n(E)$ and set $\alpha = \inf_{n>0} \frac{a_n}{n}$. From the above argument, it follows that $a_{n+m} \leq a_n + a_m$ for any $n, m \in \mathbb{N}$. Induction gives $a_n \leq n a_1, n \in \mathbb{N}$.

For $\epsilon > 0$, let $m \in \mathbb{N}$ be such that $\frac{a_m}{m} < \alpha + \frac{\epsilon}{2}$. Further choose $N \in \mathbb{N}$ to make $\frac{m}{N} < \frac{\epsilon}{2a_1}$. Then, for $n > N$, use the Division algorithm to write $n = mq + r, r < n$ or $r = 0$. This gives

$$\alpha < \frac{a_n}{n} = \frac{a_{m1+r}}{n} \tag{6.5}$$

Seeing that

$$a_{mq} \leq \underbrace{a_m + \ldots + a_m}_{q} = q a_m,$$

we that (6.5) is in turn bounded above by

$$\begin{aligned}\frac{q a_m + a_r}{n} &= \frac{a_m}{m}\frac{mq}{n} + \frac{a_r}{n} \\ &< \frac{a_m}{m} + \frac{r a_1}{n} \\ &< \alpha + \epsilon.\end{aligned}$$

□

That the same result holds for $\widetilde{\mu}_n(E)$ is obvious from the proof. Finally, we prove:

Theorem 6.2.1. *Let $E \subset \mathbb{C}$ be compact. Then*

$$\Delta(E) = \mu(E) = \widetilde{\mu}(E)$$

Proof. First, note that if $\#(E)$ is finite and $n > \#(E)$, then we can always find a polynomial $p_n \in \mathbb{C}_n[x]$ with $p_n(z) = 0$ whenever $z \in E$ (by using Lagrange interpolation, for example). Similarily, $\Delta_n(E) = 0$, as we are forced to repeat points on the product. Thus, we may assume that E contains infinitely many points.

We begin by noting that $\mu(E) \leq \widetilde{\mu}(E)$. It is further clear from the proof of Lemma 6.2.1 that $\widetilde{\mu}(E) \leq \Delta(E)$ (as the Fekete Polynomial q_n has all its roots in E). What remains to be shown is that $\Delta(E) \leq \mu(E)$.

Take $p \in \mathbb{C}_n^*[x]$ and considering the expansion of $\Delta_{n+1}(E)^{\frac{1}{2}}$ as a Vandermonde Determinant:

$$\begin{aligned}\Delta_{n+1}(E)^{\frac{1}{2}} &= \operatorname{abs}\begin{vmatrix} 1 & z_1 & \dots & z_1^{n-1} & z_1^n \\ 1 & z_2 & \dots & z_2^{n-1} & z_2^n \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & z_{n+1} & \dots & z_{n+1}^{n-1} & z_{n+1}^n \end{vmatrix} \\ &= \operatorname{abs}\begin{vmatrix} 1 & z_1 & \dots & z_1^{n-1} & p(z_1) \\ 1 & z_2 & \dots & z_2^{n-1} & p(z_2) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & z_{n+1} & \dots & z_{n+1}^{n-1} & p(z_{n+1}) \end{vmatrix}\end{aligned}$$

where the second expression is obtained by applying column-operations to the first. Expanding this with respect to the last column and denoting by $M_{i,j}$ the $(i,j)^{th}$ minor of the matrix, we get

$$\begin{aligned}\Delta_{n+1}(E)^{\frac{1}{2}} &= (-1)^{n-1}\left(p(z_1)M_{1,n+1} - p(z_2)M_{2,n+1} + \ldots + (-1)^{n-1}M_{n+1,n+1}\right)\\ &\leq \Delta_n(E)^{\frac{1}{2}} \sum_{j=1}^{n+1} |p(z_j)|\\ &\leq (n+1)\Delta_n(E)^{\frac{1}{2}} \|p\|_E . \end{aligned} \tag{6.6}$$

To simplify notation, set

$$\begin{aligned} c_n &= \left((n+1)^2 \mu_n(E)^2\right)^{\frac{1}{n}}\\ d_n &= \Delta_n(E)^{\frac{1}{n(n-1)}}. \end{aligned}$$

Then taking the infimum over all $p \in \mathbb{C}_n^*[x]$ in (6.6), the inequality, expressed with this notation, simply reads

$$d_{n+1}^{n+1} \leq c_n d_n^{n-1}.$$

Multiplying this for $n = 1, \ldots, k$ and simplifying (the assumption that E contains infinitely many points guarantees $c_n, d_n \in \mathbb{R}_{>0}$), we get

$$\begin{aligned} d_2 d_3 \cdots d_{k+1}^{k+1} &\leq c_1 c_2 \cdots c_k\\ (d_2 d_3 \cdots d_k)^{\frac{1}{k-1}} d_{k+1}^{\frac{k+1}{k-1}} &\leq c_1^{\frac{1}{k-1}} (c_2 \cdots c_k)^{\frac{1}{k-1}}. \end{aligned}$$

Note that the left is the geometric mean of the $d_i, i = 2, \ldots, k$ multiplied by an extra term, whereas the right is the geometric mean of the $c_i, i = 2, \ldots, k$. Noting that $\lim_{k\to\infty} d_k = \Delta(E)$ and $\lim_{k\to\infty} c_k = \mu(E)^2$, together with the fact that the geometric means will tend to $\Delta(E)$, $\mu(E)$, respectively, we get that

$$\Delta(E)^2 \leq \mu(E)^2$$

and the result follows, as $\Delta(E), \mu(E) \geq 0$. □

Now, consider the case $E = I = [a, b] \subset \mathbb{R}$. Using the definition of the n^{th} Chebyshev polynomial in (6.1), we will prove that $\widetilde{T_n}(x)$, defined in (6.2), indeed attains $t(I) = \frac{b-a}{4}$.

From the same expression, it is easy to see the n^{th} Chebyshev polynomial $T_n(x)$ has n real zeros at

$$x_k = \cos\left(\frac{(2k+1)\pi}{2n}\right),\ k = 0,\ldots,n-1$$

all inside the interval $[-1,1]$, and has n extrema at

$$y_k = \cos\left(\frac{k\pi}{n}\right),\ k = 0,\ldots,n-1.$$

Also, one easily sees that $T_n(y_k) = (-1)^k$, so that the polynomial equioscillates $n+1$ times between ± 1 in the interval $[-1,1]$. This gives the following result:

Theorem 6.2.2.

$$\inf_{p_n \in \mathbb{Z}_n^*[x]} \|p_n\|_{[-1,1]} = 2^{1-n}\ \|T_n\|_{[-1,1]} = 2^{1-n}$$

and $T_n(x)$ is the unique polynomial attaining this infimum.

Proof. Suppose that $q_n(x) \in \mathbb{C}_n[x]$ is a monic polynomial satisfying

$$\|q_n\|_{[-1,1]} \leq 2^{1-n} \tag{6.7}$$

and consider $s(x) = 2^{1-n}T_n(x) - \Re(q_n(x)) \in \mathbb{R}_{n-1}[x]$. Since $2^{1-n}T_n(x)$ takes on all values in $[-2^{1-n}, 2^{1-n}]$ between any two consecutive extrema, $T_n(x) = \Re(q_n(x))$ in the interval $\left[\cos\frac{k\pi}{n}, \cos\frac{(k+1)\pi}{n}\right]$ for $k = 0,\ldots,n-1$. This makes $s(x) = 0$ at least n times in $[-1,1]$. As $\partial s = n-1$, $s(x) \equiv 0$.

Now, when $T_n(x) = \pm 1$, (6.7) tells us that $q_n(x)$ is real. Thus, we have n points on $s(x)$ given, which uniquely defines $s(x)$ (using Lagrange interpolation, for example) and shows that $q_n(x)$ indeed has real coefficients, making

$$2^{1-n}T_n(x) \equiv q_n(x),\ \text{for all} x \in \mathbb{R}$$ □

This can immediately be generalised to give the following:

Corollary 6.2.3. *Let $I = [a,b] \subset \mathbb{R}$ be of finite length, $n \in \mathbb{N}$. Then*

$$t_n(I) = \|\widetilde{T_n}\|_I^{\frac{1}{n}} = \frac{b-a}{4} 2^{\frac{1}{n}}$$

where $\widetilde{T_n}(x)$ is as in (6.2).

Chapter 7

Regions where $\mathscr{S}_I$ is dense

In this chapter, we will, for a some $I \subset \mathbb{R}$, find subintervals of $(1,\infty)$ where the spectrum $\mathscr{S}_I$ is dense. We start with a description of Robinson's Method, which allows us, for large $n \in \mathbb{N}$, to find a polynomial in $\mathbb{Z}_n^*(I)$ by approximating the n^{th} Chebyshev polynomial on this interval.

We then prove that $\mathscr{S}_I$ in $(l(I),\infty)$, where $l(I) = \max\left\{1, \frac{4}{|I|}\right\}$, improving this result for intervals of the form $I_b = [0,b], b \in \mathbb{R}_{>0}$ in general, and $I = [0,1]$ in particular.

In the case of $[0,1]$, we will show how to construct a sequence of polynomials with all roots in the interval and use a modification of this sequence to prove that $\mathscr{S}_{[0,1]}$ is dense in (l,∞), where l is a limit point obtained from the sequence of polynomials. We will then mention how this result can be generalised to a larger class of intervals.

7.1 Regions of density of $\mathscr{S}_{I_b}$ for $I_b = [0,b], b \in \mathbb{R}$

7.1.1 More on Chebyshev polynomials

Let $I = [0,b], b \in \mathbb{R}_{>0}$. In this section, we will use the regular Chebyshev polynomials from (6.1), together with a method introduced by Robinson, to find a subinterval of $(1,\infty)$ where the spectrum $\mathscr{S}_I$ is dense.

We start with some definitions and motivation. In the introduction, for $n \in \mathbb{N}$, we defined the n^{th} Chebyshev polynomial $T_n(x)$ on $[-1,1]$ as the unique polynomial

solving the minimisation problem

$$\inf_{p_{n-1}\in\mathbb{C}_{n-1}[x]} \|x^n - p_{n-1}\|_{[-1,1]} = 2^{1-n}\,\|T_n\|_{[-1,1]}\,.$$

The proof relied on the fact that, for $n\in\mathbb{N}$, $T_n(x)$ equioscillates n times between ±1 on $[-1,1]$. We will make use of this equioscillation again later.

For reference, we make note of the following basic lemma:

Lemma 7.1.1. *Let $p_1,\dots,p_n$ be polynomials in $\mathbb{R}[x]$ and let $P\in\mathbb{R}[x_1,\dots,x_n]$. If the relation $P(p_1,p_2,\dots,p_n)=0$ on a set S of more than $\partial P\max_i \partial p_i$ distinct points on the real line, then $P(p_1,\dots,p_n)=0$ on all of $\mathbb{R}$.*

Proof. This follows simply from the fact that $P(p_1,\dots,p_n)$ is a univariate polynomial of degree at most $\partial P\max_i \partial p_i$. If this polynomial vanishes on S, it has to be equivalently zero. □

We will also need the following three-term recursion for $T_n(x)$:

Lemma 7.1.2. *Let $T_0(x)=1$, $T_1(x)=x$. For $n\geq 2$, the n^{th} Chebyshev polynomial $T_n(x)$ satisfies*

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x),\ \textit{for all}\ x\in\mathbb{R} \tag{7.1}$$

Proof. For $A,B\in\mathbb{R}$, we have

$$2\cos A\cos B = \cos(A-B)+\cos(A+B). \tag{7.2}$$

Let $\theta\in\mathbb{R}$, $n\in\mathbb{N}$, and set $A=(n-1)\theta$, $B=\theta$. Then, (7.2) turns into

$$2\cos\theta\cos(n-1)\theta = \cos n\theta + \cos(n-2)\theta.$$

Setting now $x=\cos\theta$, we have the desired relation, which extends to $\mathbb{R}$, as it holds on all of $[-1,1]$. □

For notational convenience, let us introduce a scaling. For $n \geq 0$, set

$$T_n^*(x) = 2T_n\left(\frac{x}{2}\right),$$

the Chebyshev polynomials scaled to the interval $[-2,2]$. The recurrence relation (7.1) then turns into

$$T_n^*(x) = xT_{n-1}^*(x) - T_{n-2}^*(x). \tag{7.3}$$

We note an important identity for $T_n^*(x)$ that can easily be proved using this relation:

Proposition 7.1.1. *For $n \in \mathbb{Z}_{\geq 0}$,*

$$T_n^*\left(x + \frac{1}{x}\right) = x^n + \frac{1}{x^n} \tag{7.4}$$

Proof. This is easily proved using induction. Seeing that $T_0^*(x) = 1+1 = 2$, $T_1^*(x+\frac{1}{x}) = x+\frac{1}{x}$, assume that $n > 1$ and that (7.4) holds for all $k < n$. Then

$$\begin{aligned} T_n^*\left(x+\frac{1}{x}\right) &= \left(x+\frac{1}{x}\right)T_{n-1}^*\left(x+\frac{1}{x}\right) - T_{n-2}^*\left(x+\frac{1}{x}\right) \\ &= \left(x+\frac{1}{x}\right)\left(x^{n-1}+\frac{1}{x^{n-1}}\right) - \left(x^{n-2}+\frac{1}{x^{n-2}}\right) \\ &= x^n + \frac{1}{x^n}. \end{aligned}$$

□

Following an argument by Robinson in [39], and using (7.3), we can find an explicit expression for the coefficients of $T_n^*(x)$.

Lemma 7.1.3. *For $n > 0 \in \mathbb{N}$,*

$$T_n^*(x) = x^n + \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} (-1)^k \frac{n}{k}\binom{n-k-1}{k-1} x^{n-2k}.$$

Proof. We will proceed by induction, using (7.3). For $n = 1,2$, the result is easily

checked. Suppose now it holds for all $k : 2 \leq k < n \in \mathbb{N}$. Then

$$\begin{aligned}
T_n^*(x) =& xT_{n-1}^*(x) - T_{n-2}^*(x) \\
=& x^n + \sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} (-1)^k \frac{n-1}{k} \binom{n-k-2}{k-1} x^{n-2k} \\
& - x^{n-2} + \sum_{k=1}^{\lfloor \frac{n-2}{2} \rfloor} (-1)^{k-1} \frac{n-2}{k} \binom{n-k-3}{k-1} x^{n-2k-2} \\
=& x^n + (n-1-1)x^{n-2} \\
& + \sum_{k=2}^{\lfloor \frac{n}{2} \rfloor} (-1)^k \left(\frac{n-1}{k} \binom{n-k-2}{k-1} + \frac{n-2}{k-1} \binom{n-k-2}{k-2} \right) x^{n-2k},
\end{aligned}$$

noting that the constant coefficient in $xT_{n-1}^*(x)$ is zero. The result follows, as

$$\begin{aligned}
& \frac{n-1}{k} \binom{n-k-2}{k-1} + \frac{n-2}{k-1} \binom{n-k-2}{k-2} \\
=& \frac{(n-1)(n-k-2)!}{k!(n-2k-1)!} + \frac{(n-2)(n-k-2)!}{(k-1)!(n-2k)!} \\
=& \frac{(n-k-2)!((n-2k)(n-1)+k(n-2))}{(n-2k)!k!} \\
=& \frac{n(n-k-1)(n-k-2)!}{k!(n-2k)!} \\
=& \frac{n}{k} \binom{n-k-1}{k-1}.
\end{aligned}$$

□

This shows that, for $n \in \mathbb{N}$, the coefficients of $T_n^*(x)$ are algebraically divisible by n – they are polynomials in n with no constant coefficient.

7.1.2 Robinson's Method

We can now use the explicit expression of $T_n^*(x)$ derived in the previous section to construct a new sequence of polynomials $p_n(x) = a_n x^n + \ldots + a_0$ which, for given $l \in \mathbb{N}$, have $a_l \ldots, a_n \in \mathbb{Z}$,as follows.

Let $c, \lambda \in \mathbb{Q}$ be fixed and set

$$P_n(x) = \lambda^n T_n^* \left(\frac{x-c}{\lambda} \right). \tag{7.5}$$

If we use Lemma 7.1.3, we see that $P_n(x)$ takes the form

$$\begin{aligned} P_n(x) &= (x-c)^n + \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} (-1)^k \frac{n}{k} \binom{n-k-1}{k-1} (x-c)^{n-2k} \lambda^{2k} \\ &= x^n + \sum_{j=1}^{n} a_j x^{n-j}, \end{aligned}$$

where the a_j are polynomials in n with $\partial_n a_j = j$ and coefficients in λ, k, c. As the coefficients of $T_n(x)$ are algebraically divisible by n, we may write the j^{th} coefficient of $P_n(x)$ as

$$a_j = \frac{\alpha_j n^j + \cdots + \alpha_1 n}{\beta_j} \tag{7.6}$$

where the $\alpha_1, \ldots, \alpha_j, \beta_j \in \mathbb{Z}$ are independent of n.

This is quite an important observation, as it yields the following lemma:

Lemma 7.1.4. *Let $\lambda, c \in \mathbb{Q}$, $l < n \in \mathbb{N}$. Then there exist infinitely many values of n such that the polynomial*

$$P_n(x) = \lambda^n T_n^*\left(\frac{x-c}{\lambda}\right) = x^n + \sum_{j=1}^{n} a_j x^{n-j}$$

has $a_0, \ldots, a_l \in \mathbb{Z}$.

Proof. In (7.6), let $m = \operatorname{lcm}\{\beta_0, \beta_1, \ldots, \beta_l\}$. Then, for $n = km$, $k \in \mathbb{N}$, $a_0, a_1, \ldots, a_l$ will be integers. □

Thus, even though the polynomial $P_n(x)$ may not have integer coefficients, for large enough n, it will be "almost integral". This is an important realisation and the main ingredient in Robinson's proof in [39] that intervals of length greater than 4 contain infinitely many complete sets of conjugate algebraic integers.

We will now show how, for given odd $A \in \mathbb{Z}$, one can approximate $P_n(x)$ by a polynomial $Q_n(x)$ with coefficients in $\frac{1}{A}\mathbb{Z}$, such that the difference $|P_n(x) - Q_n(x)|$ is small.

Lemma 7.1.5. *Let $m \in \mathbb{N}$, $A \equiv 1 \pmod 2$ be fixed, $P_n(x)$ be as above, with $c, \lambda \in \mathbb{Q}$, with $n \equiv 0 \pmod 2$ large enough so that $a_0, \ldots, a_l$ are even integers. Then one can find*

$b_k \in \left(-\frac{1}{A}, \frac{1}{A}\right]$ *such that the polynomial* $AQ_n(x)$ *with*

$$Q_n(x) = P_n(x) + \sum_{k=l+1}^{n} b_k P_{n-k}(x) \in \tfrac{1}{A}\mathbb{Z}_n[x] \tag{7.7}$$

is irreducible and has integer coefficients.

Proof. Let

$$\begin{aligned} Q_n(x) &= c_0 + \ldots + x^n \\ P_{n-k}(x) &= a_{n,k} + \ldots + a_{k+1,k}x^{n-k-1} + x^{n-k}. \end{aligned}$$

Then comparing coefficients in (7.7) yields the system of equations

$$\begin{aligned} c_0 &= a_{n,0} + b_{l+1}a_{n,l+1} + \ldots + b_{n-1}a_{n,n-1} + 2b_n \\ c_1 &= a_{n-1,0} + b_{l+1}a_{n-1,l+1} + \ldots + b_{n-2}a_{n-1,n-2} + b_{n-1} \\ &\vdots \\ c_{n-l-2} &= a_{l+2,0} + b_{l+1}a_{l+2,l+1} + b_{l+2} \\ c_{n-l-1} &= a_{l+1,0} + b_{l+1} \\ c_{n-l} &= a_{l,0} \\ &\vdots \\ c_n &= a_{0,0} = 1, \end{aligned}$$

noting that $a_{k,k} = 1$ for $0 \le k < n$ and $a_{n,n} = P_0(x) = 2$.

Consider now the equation for c_{n-l-1}. Clearly, the interval $\left(a_{l+1,0} - \frac{1}{A}, a_{l+1,0} + \frac{1}{A}\right]$ contains some $\frac{j_1}{A}$ where j_1 is an even integer. Choose $c_{n-l-1} = \frac{j_1}{A}$. This will determine the value of b_{l+1}. Given b_{l+1}, we can then choose $a_{l+2,0}, a_{l+2,l+1}$ in such a way that $c_{n-l-2} = \frac{j_2}{A}$ with $j_2 \equiv 0 \pmod 2$. Continuing in this fashion, we obtain c_{n-i}, $i = 0, \ldots, l+1$ all of the form $\frac{j_i}{A}$, $j_i \equiv 0 \pmod 2$. Seeing that, for $i > l+1$, c_{n-i} is an even integer as well, we get a polynomial $Q_n(x)$ such that $AQ_n(x)$ has even integer coefficients. The first equation (obtained using $P_0(x) = 2$) further allows us to choose $Ac_0 \equiv 2 \pmod 4$, so that $AQ_n(x)$ will be irreducible by Eisenstein's criterion. □

We have thus successfully approximated the polynomial $P_n(x)$ by an irreducible

polynomial with coefficients in $\frac{1}{A}\mathbb{Z}$. More can be said, however. First, note that $\|P_n\|_{[c-2\lambda,c+2\lambda]} = 2\lambda^n$. Now, take $\lambda > 1$ and choose $l \in \mathbb{N}$ such that $\lambda^l(\lambda-1) \geq 1$. Then, for n chosen as in Lemma 7.1.5, we have

$$\begin{aligned}|P_n(x) - Q_n(x)| &= \left|\sum_{k=l+1}^{n} b_k P_{n-k}(x)\right| \\ &\leq \sum_{k=l+1}^{n} |b_k||P_{n-k}(x)| \\ &< \sum_{k=l+1}^{\infty} 2\lambda^{n-k} = \frac{2\lambda^n}{\lambda^l(\lambda-1)} \leq 2\lambda^n\end{aligned}$$

Since $P_n(x)$ equioscillates n times between $\pm 2\lambda^n$ on $[c-2\lambda, c+2\lambda]$, $Q_n(x)$ has the same sign as $P_n(x)$ at the extrema of $P_n(x)$ – thus changing sign n times in $[c-2\lambda, c+2\lambda]$. Consequently, $Q_n(x) \in \frac{1}{A}\mathbb{Z}_n(I)$, and therefore $AQ(x) \in \mathbb{Z}_n(I)$.

7.1.3 Dense regions of $\mathscr{S}_I$ for arbitrary $I \subset \mathbb{R}$

We start with an arbitrary interval $I = [a,b]$ and show how Lemma 7.1.5 can be used to prove results about the spectrum $\mathscr{S}_I$.

Theorem 7.1.1. *Let $I = [a,b] \subset \mathbb{R}$ be an interval of length $0 < |I| < 4$. Then $\mathscr{S}_I$ is dense in $\left(\frac{4}{|I|}, \infty\right)$.*

Proof. Let $[a,b] = [c-2\lambda, c+2\lambda]$, so that $\frac{|I|}{4} = \lambda$ and let $\alpha \in \left(\frac{1}{\lambda}, \infty\right)$.

For $0 < \epsilon < \alpha - \frac{1}{\lambda}$, we see that $\alpha - \epsilon > \frac{1}{\lambda}$, so that there exists $n_1 \in \mathbb{N}$ with

$$((\alpha-\epsilon)\lambda)^{n_1} > \frac{1}{1-\lambda}.$$

Further, we may choose $n_2 \in \mathbb{N}$ with

$$\left(\frac{\alpha+\epsilon}{\alpha-\epsilon}\right)^{n_2} > 3.$$

Note that, since $\lambda < 1$, $\alpha - \epsilon > \frac{1}{\lambda} > 1$, so that

$$\begin{aligned}(\alpha+\epsilon)^{n_2} &> (\alpha-\epsilon)^{n_2} + 2(\alpha-\epsilon)^{n_2} \\ &> (\alpha-\epsilon)^{n_2} + 2\end{aligned}$$

Taking $n = \max\{n_1, n_2\}$, we get consecutive integers $s, s+1$ with

$$\left(\frac{1}{\lambda}\right)^n \frac{1}{1-\lambda} < (\alpha-\epsilon)^n < s < s+1 < (\alpha+\epsilon)^n.$$

Let A be the odd one of $s, s+1$. Then, following the argument in Lemma 7.1.5 with $l = 0$, we may choose $b_1, \ldots, b_n \in \left(-\frac{1}{A}, \frac{1}{A}\right]$ such that $Q_n(x) = P_n(x) + \sum_{k=1}^{n} b_k P_{n-k}(x)$ is irreducible and $AQ_n(x)$ has integer coefficients. We also get

$$\begin{aligned} |P_n(x) - Q_n(x)| &= \left|\sum_{k=1}^{n} b_k P_{n-k}(x)\right| \\ &\leq \frac{1}{A}\sum_{k=1}^{n} 2\lambda^{n-k} = \frac{2}{A}\sum_{j=0}^{n-1}\lambda^j \\ &\leq \frac{2}{A}\sum_{j=0}^{\infty}\lambda^j = \frac{2}{A(1-\lambda)} \\ &< 2\lambda^n. \end{aligned}$$

Thus, by the same argument as used at the end of Section 7.1.2, $Q_n(x)$ (and consequently $AQ_n(x)$) will have all its roots in I and

$$|\alpha - A^{1/n}| < \epsilon. \qquad \square$$

7.1.4 Application to the spectrum of I_b

Now, let $Q_n(x)$ be as in Lemma 7.1.5, but with $A = 1$. Set $R_n(x) = x^n Q_n(\frac{1}{x})$. Clearly, $R_n(x)$ now has all its roots in the interval $\left[\frac{1}{c+2\lambda}, \frac{1}{c-2\lambda}\right]$. We have the following:

Lemma 7.1.6. *Let a_n denote the leading coefficient of $R_n(x)$. Then*

$$\lim_{n\to\infty} |a_n|^{\frac{1}{n}} = \frac{1}{2}\lambda\left(c + \sqrt{c^2 - 4\lambda^2}\right). \tag{7.8}$$

Proof. To begin with, let $c, \lambda \in \mathbb{Q}$ with $\lambda > 1$ and $c > 2\lambda$. Set

$$\gamma = -\frac{c + \sqrt{c^2 - 4\lambda^2}}{2}, \tag{7.9}$$

a solution to $\gamma + \gamma^{-1} = -\frac{c}{\lambda}$. Note that with $c > 1, c^2 - 4\lambda^2 \geq 0$, giving $|\gamma| > 1$. Thus,

choose $l \in \mathbb{N}$ such that

$$(|\gamma|\lambda)^l(|\gamma|\lambda - 1) > 2. \tag{7.10}$$

Choose n such that, in the notation of Lemma 7.1.4, n is a multiple of $m = \operatorname{lcm}\{2, \beta_0, \beta_1, \ldots, \beta_l\}$. Recalling that $T_n^*\left(x + \frac{1}{x}\right) = x^n + \frac{1}{x^n}$, we get

$$\begin{aligned} a_n = Q_n(0) &= P_n(0) + \sum_{k=l+1}^{n} b_k P_{n-k}(0) \\ &= \lambda^n T_n^*\left(-\frac{c}{\lambda}\right) + \sum_{k=l+1}^{n} b_k \lambda^{n-k} T_{n-k}^*\left(-\frac{c}{\lambda}\right) \\ &= \lambda^n(\gamma^n + \gamma^{-n}) + \sum_{k=l+1}^{n} b_k \lambda^{n-k}(\gamma^{n-k} + \gamma^{k-n}) \\ &= (\lambda\gamma)^n\left(1 + \gamma^{-2n} + \sum_{k=l+1}^{n} b_k \lambda^{-k}(\gamma^{-k} + \gamma^{k-2n})\right). \end{aligned}$$

Consider now the last term of this expression. Taking the limit over the subsequence $n = sm, s \in \mathbb{N}$, we get

$$\begin{aligned} \lim_{n\to\infty}\left|\sum_{k=l+1}^{n} b_k \lambda^{-k}\left(\gamma^{-k} + \gamma^{k-2n}\right)\right| &\le \lim_{n\to\infty}\left(\sum_{k=l+1}^{n} |b_k||\lambda\gamma|^{-k} + \sum_{k=l+1}^{n} |b_k||\gamma|^{k-2n}|\lambda|^{-k}\right) \\ &< 2\sum_{k=l+1}^{\infty} |\lambda\gamma|^{-k} = \frac{2}{|\lambda\gamma|^l(\lambda\gamma - 1)} < 1. \end{aligned}$$

Thus, we get

$$\lim_{n\to\infty}\left(1 + \gamma^{-2n} + \sum_{k=l+1}^{n} b_k \lambda^{-k}(\gamma^{-k} + \gamma^{k-2n})\right) = 1 + A,$$

where $|A| < 1$, making the limit nonzero and finite. This gives

$$\begin{aligned} \lim_{n\to\infty} |b_n|^{\frac{1}{n}} &= \lim_{n\to\infty} |\lambda\gamma|\left|1 + \gamma^{-2n} + \sum_{k=l+1}^{n} b_k \lambda^{-k}(\gamma^{-k} + \gamma^{k-2n})\right|^{\frac{1}{n}} \\ &= |\lambda\gamma| \\ &= \frac{1}{2}\lambda\left(c + \sqrt{c^2 - 4\lambda^2}\right). \end{aligned}$$

□

Corollary 7.1.2. *Let $c, \lambda \in \mathbb{R}$, $\lambda > 1, c > 2\lambda$. Then there exists a sequence of irreducible*

polynomials $\{p_n\}$*, where* $p_n \in \mathbb{Z}_n\left(\left[\frac{1}{c+2\lambda}, \frac{1}{c-2\lambda}\right]\right)$ *has leading coefficient* a_n*, with*

$$\lim_{n\to\infty} |a_n|^{\frac{1}{n}} = \frac{1}{2}\lambda\left(c + \sqrt{c^2 - 4\lambda}\right).$$

Proof. The argument above shows this for intervals with rational endpoints. What remains to be shown is that this extends to intervals with irrational endpoints as well.

Let $\{c_i\}, \{\lambda_i\}$ be sequences of rationals such that, for $i \in \mathbb{N}$, $\lambda_i > 1, c_i > 2\lambda_i$, and also

$$I_i = \left[\frac{1}{c_i + 2\lambda_i}, \frac{1}{c_i - 2\lambda_i}\right] \subset \left[\frac{1}{c+2\lambda}, \frac{1}{c-2\lambda}\right]$$

and $\lim_{i\to\infty} c_i = c, \lim_{i\to\infty} \lambda_i = \lambda$. Certainly, any polynomial having all roots in I_i will also have all roots in I and further,

$$\lim_{i\to\infty} \frac{1}{2}\left(c_i + \sqrt{c_i^2 - 4\lambda_i^2}\right) = \frac{1}{2}\left(c + \sqrt{c^2 - 4\lambda^2}\right),$$

by continuity. □

We can now prove the following corollary, telling us a lot about the structure of $\mathscr{S}_{[0,b]}$:

Corollary 7.1.3. *Let* $I_b = [0, b], b \in \mathbb{R}_{>0}$*. Then the spectrum* $\mathscr{S}_{I_b}$ *is dense in* (l_b, ∞)*, where*

$$l_b = 1 + \frac{1}{2b}\left(1 + \sqrt{1 + 4b}\right).$$

Proof. This follows as a simple corollary from the previous results. For the given $b \in \mathbb{R}$, choose $c, \lambda \in \mathbb{R}$ with

$$\frac{1}{c - 2\lambda} = b \tag{7.11}$$

and $\lambda > 1, c \geq 2\lambda$. Now let $\epsilon > 0$ and choose

$$\lambda = 1 + \frac{\epsilon}{2}$$
$$c = 2\lambda + \frac{1}{b} = 2 + \frac{1}{b} + \epsilon.$$

We get a sequence of polynomials with all roots in the interval

$$\left[\frac{1}{c+2\lambda}, \frac{1}{c-2\lambda}\right] = \left[\frac{1}{4+2\epsilon+\frac{1}{b}}, b\right] \subset [0, b]$$

and leading coefficients a_n satisfying

$$\lim_{n\to\infty} |a_n|^{\frac{1}{n}} = l(b,\epsilon).$$

where $l(b,\epsilon)$ is a monotone increasing continuous function with $\lim_{\epsilon\to\infty} l(b,\epsilon) = \infty$ and

$$\lim_{\epsilon\to 0} l(b,\epsilon) = 1 + \frac{1}{2b}\left(1+\sqrt{1+4b}\right). \qquad \square$$

7.2 Special cases

For certain intervals, the results of the previous sections can be improved. Here, one can use a particular sequence of polynomials with all roots on the positive real line and small leading coefficients, and modify this sequence to obtain polynomials with all roots in these intervals with rational endpoints whose normalised leading coefficients are dense within a certain subset of $[1,\infty)$.

These so-called Gorškov polynomials were first defined by Gorškov in [23], and later rediscovered by Smyth in [42]. Wirsing, in 1981, unaware of Gorškov's earlier work, defined the polynomials independently for $[0,1]$ – which is why they are often referred to as Gorškov-Wirsing polynomials in the literature. More details on the construction following his method can be found in [35], as well as the appendix on the polynomials in [20]. More on these polynomials can also be found in [7].

7.2.1 The Gorškov polynomials

We will start by constructing a sequence of polynomials with all roots on the real line through a recursive process. Let $p_0(x) = x - 1$ and define a sequence $\{p_k(x)\}_{k=0}^{\infty}$

recursively by

$$p_k(x) = x^{2^{k-1}} p_{k-1}\left(x - \frac{1}{x}\right). \tag{7.12}$$

Lemma 7.2.1. *The Gorškov polynomials $p_k(x) \in \mathbb{Z}(\mathbb{R})$, defined above, have the following properties:*

1. *$p_k(x)$ is monic and of degree 2^k*

2. *$p_k(x)$ has all roots on the real line.*

Proof. That $p_k(x)$ is monic follows straight from the definition, as $p_0(x)$ is monic and the recursive relation does not change the leading coefficient. Similar, it is clear that the degree of $p_k(x)$ is 2^k just by noticing that each step in the recusion doubles the degree of the polynomial.

It becomes clear that all elements of the sequence have all their roots on the real line if we look at the corresponding recurrence relation for the roots. We let $\beta_0 = 1$ and get

$$\beta_k - \beta_k^{-1} = \beta_{k-1}, \tag{7.13}$$

so that β_k is a zero of the quadratic $x^2 - x\beta_{k-1} - 1$ over $\mathbb{Q}(\beta_{k-1})$ with determinant $\beta_{k-1}^2 + 4 > 0$ for real β_{k-1}, making β_k real if β_{k-1} is. Seeing now that $\beta_0 = 1$ is real, the result follows by induction. □

In [35], the Gorškov polynomials are defined differently. Consider the iterates of $v(x) = x - \frac{1}{x}$. If we start writing out the first few iterates,

$$\begin{aligned} v(x) &= x - \frac{1}{x} = \frac{x^2-1}{x} \\ v^{(2)}(x) &= \frac{x^2-1}{x} - \frac{x}{x^2-1} = \frac{(x^2-1)^2 - x^2}{x(x^2-1)}. \end{aligned} \tag{7.14}$$

it soon becomes clear that $v^{(k)}(x)$ will be of the form

$$v^{(k)}(x) = \frac{g_{k-1}(x^2)}{x h_{k-1}(x^2)} \tag{7.15}$$

with $g_{k-1}, h_{k-1} \in \mathbb{Z}[x]$.

Lemma 7.2.2. *Let $v(x)$ as in (7.14). Then, for $k \geq 0$,*

$$v^{(k+1)}(x) = \frac{g_k(x^2)}{x h_k(x^2)},$$

where $\gcd(g_k, h_k) = 1$ *with* $g_0(x) = x - 1, g_1(x) = x^2 - 3x + 1$ *and*

$$\begin{aligned} g_k(x) &= g_{k-1}^2(x) + g_{k-1}(x) g_{k-2}^2(x) - g_{k-2}^4(x), \ k \geq 2 \\ h_k(x) &= \prod_{i=0}^{k-1} g_i(x), \ k \geq 1. \end{aligned} \tag{7.16}$$

Proof. We will proceed by induction on k. The case $k = 0$ follows from (7.14).

Suppose now the result holds for all $j \leq k$ and consider

$$\begin{aligned} v^{(k+1)}(x) &= \frac{g_{k-1}(x^2)}{x h_{k-1}(x^2)} - \frac{x h_{k-1}(x^2)}{g_{k-1}(x^2)} \\ &= \frac{g_{k-1}^2(x^2) - x^2 h_{k-1}^2(x^2)}{x h_{k-1}(x^2) g_{k-1}(x^2)}. \end{aligned}$$

Now, since $\gcd(g_{k-1}, h_{k-1}) = 1$, it follows that $\gcd(g_{k-1}^2 - x^2 h_{k-1}^2, x g_{k-1} h_{k-1}) = 1$, so that, upon equating numerators and denominators, we obtain

$$g_k(x^2) = g_{k-1}^2(x^2) - x^2 h_{k-1}^2(x^2) \tag{7.17}$$

$$h_k(x^2) = g_{k-1}(x^2) h_{k-1}(x^2). \tag{7.18}$$

From (7.18), the expression for $h_k(x)$ follows by induction. To obtain (7.16), note that for $k \geq 2$,

$$x^2 h_{k-1}(x^2) = g_{k-2}^2(x^2) - g_{k-1}(x^2)$$

from (7.17) with k replaced by $k - 1$. Then

$$\begin{aligned} g_k(x^2) &= g_{k-1}^2(x^2) - g_{k-2}^2(x^2) \left(g_{k-2}^2(x^2) - g_{k-1}(x^2) \right) \\ &= g_{k-1}^2(x^2) + g_{k-1}(x^2) g_{k-2}^2(x^2) - g_{k-2}^4(x^2). \end{aligned}$$

□

Not surprisingly, these polynomials actually produce the same polynomials as defined in (7.12), as the following lemma shows:

Lemma 7.2.3. *Let $k \geq 1$, $p_k(x)$, $g_k(x)$ be defined as in (7.12), (7.15), respectively. Then $g_{k-1}(x^2) = p_k(x)$ for all $k \in \mathbb{N}$.*

Proof. We begin by writing $p_k(x)$ as

$$\begin{aligned} p_k(x) &= x^{2^{k-1}} p_{k-1}(v(x)) \\ &= x^{2^{k-1}} v(x)^{2^{k-2}} p_{k-2}\left(v^{(2)}(x)\right) \\ &= \cdots \\ &= x^{2^{k-1}} \left(\prod_{j=1}^{k-1} v^{(j)}(x)^{2^{k-j-1}}\right)\left(v^{(k)}(x) - 1\right). \end{aligned} \tag{7.19}$$

By using (7.15) for $j = 1, \ldots, k-1$, we get that the right-hand side is actually

$$\begin{aligned} & x^{2^{k-1}} \left(\frac{g_0(x^2)}{x}\right)^{2^{k-2}} \left(\frac{g_1(x^2)}{x g_0(x^2)}\right)^{2^{k-3}} \cdots \left(\frac{g_{k-2}(x^2)}{x g_0(x^2) \cdots g_{k-3}(x^2)}\right) v^{(k)}(x) \\ =& x g_0(x^2) g_1(x^2) \cdots g_{k-2}(x^2)\left(v^{(k)}(x) - 1\right) \\ =& x h_{k-1}(x^2)\left(v^{(k)}(x) - 1\right). \end{aligned}$$

Rearranging then gives

$$v^{(k)}(x) = \frac{p_k(x) + x h_{k-1}(x^2)}{x h_{k-1}(x^2)}.$$

Noting that the denominator of this equals $g_{k-1}(x^2)$, we get

$$g_{k-1}(x^2) = p_k(x) + x h_{k-1}(x^2),$$

so that

$$\begin{aligned} p_k(x) p_k(-x) &= \left(g_{k-1}(x^2) - x h_{k-1}(x^2)\right)\left(g_{k-1}(x^2) + x h_{k-1}(x^2)\right) \\ &= g_{k-1}^2(x^2) - x^2 h_{k-1}^2(x^2) \\ &= g_k(x^2), \end{aligned}$$

by using (7.17). □

The $g_k(x)$ now have all roots on the positive real line, and satisfy a similar recurrence relation: for $k \geq 1$,

$$\begin{aligned} g_k(x) &= p_k\left(\sqrt{x}\right) p_k\left(-\sqrt{x}\right) \\ &= x^{2^{k-1}} p_{k-1}\left(v\left(\sqrt{x}\right)\right) p_{k-1}\left(v\left(-\sqrt{x}\right)\right) \\ &= x^{2^{k-1}} p_{k-1}\left(v\left(\sqrt{x}\right)\right) p_{k-1}\left(-v\left(\sqrt{x}\right)\right) \\ &= x^{2^{k-1}} g_{k-1}\left(\left(v\left(\sqrt{x}\right)\right)^2\right) \\ &= x^{2^{k-1}} g_{k-1}\left(x+\tfrac{1}{x}-2\right). \end{aligned} \tag{7.20}$$

7.2.2 Gorškov polynomials for $[0,1]$

Using the polynomials defined in the previous section, we can create a sequence $\{r_k\}_{k=1}^{\infty}$ of polynomials with all roots in $[0,1]$ by letting

$$r_k(x) = x^{2^k} g_k\left(\frac{1}{x}-1\right). \tag{7.21}$$

This has the same effect as applying the transformation $\tau(x) = \frac{1}{1+x}$ to the β_k.

One then obtains a sequence of polynomials satisfying the following:

Lemma 7.2.4. *Let*

$$u(x) = \frac{x(1-x)}{1-3x(1-x)}. \tag{7.22}$$

The k^{th} Gorškov polynomial $r_k(x)$ on $[0,1]$ is defined recursively by

$$\begin{aligned} r_0(x) &= 1-2x \\ r_k(x) &= (-1+3x(1-x))^{2^{k-1}} r_{k-1}(u(x)), \quad k \geq 1 \end{aligned} \tag{7.23}$$

Proof. Using (7.20), together with the definition for $r_k(x)$,

$$\begin{aligned} r_k(x) &= x^{2^k} g_k\left(\frac{1}{x}-1\right) \\ &= x^{2^k}\left(\frac{1}{x}-1\right)^{2^{k-1}} g_{k-1}\left(\frac{(2x-1)^2}{x(1-x)}\right) \\ &= (x(1-x))^{2^{k-1}}\left(\frac{1-3x(1-x)}{x(1-x)}\right)^{2^{k-1}} r_{k-1}\left(\frac{x(1-x)}{1-3x(1-x)}\right) \\ &= (-1+3x(1-x))^{2^{k-1}} r_{k-1}\left(\frac{x(1-x)}{1-3x(1-x)}\right). \end{aligned}$$

□

Using these polynomials, we get the following (taken from [35]):

Theorem 7.2.1. *The polynomials $r_k(x) \in \mathbb{Z}_{2^k}[x]$, defined above, are irreducible over $\mathbb{Q}$.*

Proof. Suppose we have some $k \in \mathbb{N}$ such that $r_k(x)$ is irreducible, but $r_{k+1}(x)$ factors. Then the equation $u(x) = \beta_k$, which can be rewritten as

$$f(x) = x^2 - x + \frac{\beta_k}{3\beta_k + 1} = 0$$

factors over $\mathbb{Q}(\beta_k)$. Since $f(x) = f(1-x)$, we then get that

$$r_{k+1}(x) = ca(x)a(1-x) \tag{7.24}$$

for some constant $c \in \mathbb{Z}$ and $a(x) \in \mathbb{Z}[x]$.

Now, as $r_0(0) = 1$ and

$$r_{k+1}(0) = r_k(u(0)) = r_k(0)\ , k \geq 0,$$

it follows that $c = 1$, so that the leading coefficient $a_{2^{k+1}}$ of $r_{k+1}(x)$ is a perfect square.

Consider now the recurrence relation (7.16). Consider now the leading coefficient a_{2^k} of $r_k(x)$:

$$\begin{aligned} a_{2^k} &= \lim_{x\to\infty} x^{2^k} r_k(x) \\ &= \lim_{x\to\infty} g_k\left(\tfrac{1}{x} - 1\right) \\ &= g_k(-1). \end{aligned}$$

Thus, by using (7.16), we get that

$$a_{2^{k+1}} = a_{2^k}^2 + a_{2^k} a_{2^{k-1}}^2 - a_{2^{k-1}}^4.$$

Seeing now that $a_1 \equiv a_2 \equiv 2 \pmod 3$, one can show by induction that $a_{2^k} \equiv 2 \pmod 3$ for all k, so that a_{2^k} cannot be a square. □

Since we are interested in the leading coefficients of these polynomials, the following Lemma is of importance:

Lemma 7.2.5. *Let $v(x) = x - \frac{1}{x}$. For $k \geq 1$, the normalised leading coefficient of $r_k(x) = a_{2^k} x^{2^k} + \ldots + a_0$ is given by*

$$\left|a_{2^k}\right|^{\frac{1}{2^k}} = \left(\prod_{j=1}^{k-1} \left|v^{(j)}(i)\right|^{\frac{1}{2^j}}\right) \left|v^{(k)}(i) - 1\right|^{\frac{1}{2^{k-1}}}$$

where $i = \sqrt{-1}$.

Proof. From (7.2.3), together with the fact that $a_{2^k} = g_k(-1)$, we get

$$|a_{2^k}| = |p_k(i)||p_k(-i)|.$$

Now, from $v(-z) = -z + \frac{1}{z} = -v(z)$ and

$$v^{(k)}(-z) \quad = \quad v^{(k-1)}(-z) - \frac{1}{v^{(k-1)}(-z)}, \quad k \geq 1$$

it is easily seen that all the iterates of $v(z)$ are odd functions in the complex variable z.

Now, as $v^{(k)}(z)$ is odd, $|v(z)| = |v(-z)|$ and we get an expression for $|a_{2^k}|$, using (7.19):

$$\begin{aligned} |a_{2^k}| &= |p_k(i)||p_k(-i)| \\ &= \left(\prod_{j=1}^{k-1} \left(\left|v^{(j)}(i)\right|^{2^{k-j-1}}\right)^2\right) \left|v^{(k)}(i) - 1\right|^2 \\ &= \left(\prod_{j=1}^{k-1} \left|v^{(j)}(i)\right|^{2^{k-j}}\right) \left|v^{(k)}(i) - 1\right|^2. \end{aligned}$$

Taking 2^k-th roots of this expression then yields the result. □

The following is an auxiliary result:

Lemma 7.2.6. *Let $b \in \mathbb{R}$, $k \in \mathbb{N}$. Then*

$$\left|v^{(k)}(i) - b\right|^2 = \left|v^{(k)}(i)\right|^2 + b^2$$

Proof. This follows from the fact that $v^{(k)}(i)$ is purely imaginary, for $k \in \mathbb{N}$, which we can show by induction: for $k = 1$, $v(i) = i - \frac{1}{i} = 2i$ is purely imaginary. At the same

time, if $v^{(k)}(i)$ is purely imaginary, then

$$v^{(k+1)}(i) = \left|v^{(k)}(i)\right| i + \frac{1}{\left|v^{(k)}(i)\right|} i \tag{7.25}$$

is purely imaginary as well. Thus,

$$\begin{aligned}\left|v^{(k)}(i) - b\right|^2 &= \left(\Im\left(v^{(k)}(i) - b\right)\right)^2 + \left(\Re\left(v^{(k)}(i) - b\right)\right)^2 \\ &= \left|v^{(k)}(i)\right|^2 + b^2.\end{aligned}$$

□

This result yields a highly important limit point in the spectrum of $[0,1]$:

Lemma 7.2.7. *The sequence* $\left\{|a_{2^k}|^{1/2^k}\right\}_{k=1}^{\infty}$ *converges to*

$$\lim_{k\to\infty} |a_{2^k}|^{\frac{1}{2^k}} = 2.37684\ldots$$

Proof. Using the expression of a_{2^k} from the previous lemma, it is clear that we have to analyse the behaviour of the sequence $\{|v^{(k)}(i)|\}_{k=1}^{\infty}$. From (7.25), it follows that

$$|v^{(k+1)}(i)| = |v^{(k)}(i)| + \frac{1}{|v^{(k)}(i)|},$$

showing that the sequence $\{|v^{(k)}(i)|\}_{k=1}^{\infty}$ is increasing.

For fixed $k \in \mathbb{N}$, using the above, we also get

$$\begin{aligned}|v^{(k)}(i)| &= |v^{(k-1)}(i)| + \frac{1}{|v^{(k-1)}(i)|} \\ &\leq |v^{(k-1)}(i)| + \frac{1}{|v(i)|} \\ &\leq |v^{(k-2)}(i) + \frac{2}{|v(i)|} \\ &\leq \cdots \\ &\leq |v(i)| + \frac{k-1}{|v(i)|}.\end{aligned} \tag{7.26}$$

Taking 2^k-th roots of both sides of this inequality, we see that $\left\{\left|v^{(k)}(i)\right|^{1/2^k}\right\}_{k=1}^{\infty}$ is a bounded sequence.

Using these results for fixed $k \in \mathbb{N}$, we have

$$\begin{aligned}
\left|v^{(k+1)}(i)\right|^{\frac{1}{2^{k-1}}} + 1 &\geq \left|v^{(k)}(i)\right|^{\frac{1}{2^{k-1}}} + 1 \\
\left|v^{(k)}(i)\right|^{\frac{1}{2^k}} \left|v^{(k+1)}(i) - 1\right|^{\frac{1}{2^{k-1}}} &\geq \left|v^{(k)}(i) - 1\right|^{\frac{1}{2^{k-1}}} \\
\left(\prod_{j=1}^{k-1} \left|v^{(j)}(i)\right|^{\frac{1}{2^j}}\right) \left|v^{(k)}(i)\right|^{\frac{1}{2^k}} \left|v^{(k+1)}(i) - 1\right|^{\frac{1}{2^{k-1}}} &\geq \left(\prod_{j=1}^{k-1} \left|v^{(j)}(i)\right|^{\frac{1}{2^j}}\right) \left|v^{(k)}(i-1)\right|^{\frac{1}{2^{k-1}}} \\
\left(\prod_{j=1}^{k} \left|v^{(j)}(i)\right|^{\frac{1}{2^j}}\right) \left|v^{(k+1)}(i) - 1\right|^{\frac{1}{2^k}} &\geq \left(\prod_{j=1}^{k-1} \left|v^{(j)}(i)\right|^{\frac{1}{2^j}}\right) \left|v^{(k)}(i) - 1\right|^{\frac{1}{2^{k-1}}},
\end{aligned}$$

proving that $|a_{2^k}|$ is an increasing sequence. At the same time, using (7.26), we see that

$$\log\left(\prod_{j=1}^{k-1} \left|v^{(j)}(i)\right|^{\frac{1}{2^j}}\right) \left|v^{(k}(i) - 1\right|^{\frac{1}{2^k}} \leq \sum_{j=1}^{k-1} \frac{1}{2^j} \log \frac{j+1}{2} + \frac{1}{2^k} \log\left(\left(\frac{k+1}{2}\right)^2 + 1\right) < \infty,$$

so that the sequence $\left\{\left|a_{2^k}^{1/2^k}\right|\right\}$ is also bounded above, ad thus converges by the monotone converge theorem.

To evaluate the limit, one may use a computer package such as MAPLE. □

7.2.3 A generalisation of the Gorškov polynomials

While the Gorškov polynomials $r_k(x)$ for $[0,1]$ are important in their own right, their definition can be modified to derive different sequences of polynomials: Let $b \equiv 1 \pmod 2$ be an integer and set

$$\begin{aligned}
p_0^{(b)}(x) &= x - b \\
p_k^{(b)}(x) &= x^{2^{k-1}} p_{k-1}^{(b)}(v(x)),\ k \geq 1,
\end{aligned}$$

where $v(x)$ is as in (7.14).

As before, we get a corresponding sequence

$$\begin{aligned}
r_0^{(b)}(x) &= (b^2+1)x - 1 \\
r_k^{(b)}(x) &= p_k^{(b)}\left(\sqrt{\tfrac{1}{x} - 1}\right) p_k^{(b)}\left(-\sqrt{\tfrac{1}{x} - 1}\right), k \geq 1.
\end{aligned}$$

with all roots in $[0,1]$. The leading coefficient $a_{2^k}^{(b)}$ of $r_k^{(b)}(x)$ are easily seen to satisfy

$$\left|a_{2^k}^{(b)}\right|^{\frac{1}{2^k}} = \left(\prod_{j=1}^{k-1}\left|v^{(j)}(i)\right|^{\frac{1}{2^j}}\right)\left|v^{(k)}(i)-b\right|^{\frac{1}{2^{k-1}}}. \tag{7.27}$$

It is worth noting that the limit $\lim_{k\to\infty}|a_{2^k}^{(b)}|^{1/2^k}$ is not affected by the change of initial root $b\in\mathbb{Z}$ of $g_k^{(b)}(x)$:

Lemma 7.2.8. *Let $r_k^{(b)}(x)$ be defined as above, $b\in\mathbb{Z}$. Then*

$$\lim_{k\to\infty}\left|a_{2^k}^{(b)}\right|^{\frac{1}{2^k}} = \lim_{k\to\infty}\left|a_{2^k}\right|^{\frac{1}{2^k}}.$$

Proof. Using Lemma 7.25, we may write the square of the normalised leading coefficient as

$$\begin{aligned}\left|a_{2^k}^{(b)}\right|^{\frac{1}{2^{k-1}}} &= \left(\prod_{j=1}^{k-1}\left|v^{(j)}(i)\right|^{\frac{1}{2^{j-1}}}\right)\left|v^{(k)}(i)\right|^{\frac{1}{2^{k-1}}}\left(1+\frac{b^2}{\left|v^{(k)}(i)\right|^2}\right)^{\frac{1}{2^k}}\\ &= \left|a_{2^k}\right|^{\frac{1}{2^{k-1}}}\left(1+\frac{b^2}{|v^{(k)}(i)|^2}\right)^{\frac{1}{2^k}}.\end{aligned} \tag{7.28}$$

The result now follows by taking limits and using the fact that $|v^{(k)}(i)|$ is bounded both below and above (see proof of Lemma 7.2.7). □

While, for any given $b\in\mathbb{N}$, the normalised leading coefficients of $r_k^{(b)}(x)$ tend to the same limit as these of the $r_k(x)$, they converge to this limit differently: For a larger choice of $b\in\mathbb{N}$, the initial leading coefficient b^2+1 will be larger as well. If we now have some $\alpha > l = \lim_{k\to\infty}|a_{2^k}|^{1/2^k}$, we can choose b large enough to produce a sequence of polynomials with a large enough initial leading coefficient so that, for an appropriate choice of k, there will be some $\left|a_{2^k}^{(b)}\right|^{1/2^k}$ arbitrarily close to α. The details of this argument are contained in the proof of the following theorem:

Theorem 7.2.2. *Let $\alpha > l = \lim_{k\to\infty}|a_{2^k}|^{1/2^k}$. Then, for any $\epsilon>0$, there are $k,b\in\mathbb{N}$ with $b\equiv 1 \pmod 2$ such that*

$$\left|\left|a_{2^k}^{(b)}\right|^{\frac{1}{2^k}}-\alpha\right| < \epsilon.$$

Proof. We will actually prove that, for any $\alpha > l, \epsilon > 0$, there exist $b, k \in \mathbb{N}$ such that

$$\left| \frac{1}{2^k} \log \left| a_{2^k}^{(b)} \right| - \log \alpha \right| < \epsilon,$$

from which the result follows by continuity of the logarithm.

Using Lemma 7.2.6, we may rewrite the square of (7.27) as

$$\left| a_{2^k}^{(b)} \right|^2 = \left(\prod_{j=1}^{k-1} \left| v^{(j)}(i) \right|^{2^{k-j+1}} \right) \left(\left| v^{(k)}(i) \right|^2 + b^2 \right).$$

Given $\alpha > l$, $\epsilon > 0$, choose $k_1 \in \mathbb{N}$ such that

$$\frac{1}{2^{k_1-1}} \log |a_{2^{k_1}}| > 2 \log l - \epsilon. \tag{7.29}$$

Further, choose $k_2 \in \mathbb{N}$ so that the interval

$$I_{k_2} = \left(|v^{(k_2)}(i)|^2 \exp\left(\left(2^{k_2} \left(2 \log \tfrac{\alpha}{l} - \epsilon \right) - 1 \right) \right), \right.$$
$$\left. |v^{(k_2)}(i)|^2 \exp\left(\left(2^{k_2} \left(2 \log \tfrac{\alpha}{l} + 2\epsilon \right) - 1 \right) \right) \right)$$

contains a perfect square b^2 with $b \equiv 1 \pmod 2$. Set $k = \max\{k_1, k_2\}$ and let b^2 lie in I_k. Then

$$2 \log \frac{\alpha}{l} - \epsilon < \frac{1}{2^k} \log \left(1 + \frac{b^2}{|v^{(k)}(i)|^2} \right) < 2 \log \frac{\alpha}{l} + 2\epsilon. \tag{7.30}$$

Taking (7.29) and (7.30) together, and using (7.28), we get

$$\begin{aligned} 2 \log l - \epsilon + 2 \log \frac{\alpha}{l} - \epsilon < & \sum_{j=1}^{k-1} \frac{1}{2^{j-1}} \log \left| v^{(j)}(i) \right| \\ & + \frac{1}{2^{k-1}} \log \left| v^{(k)}(i) \right| + \frac{1}{2^k} \log \left(1 + \frac{b^2}{|v^{(k)}(i)|^2} \right) \\ < & 2 \log l + \left(2 \log \frac{\alpha}{l} + 2\epsilon \right) \end{aligned}$$

so that

$$\log \alpha - \epsilon < \log \left(\prod_{j=1}^{k-1} |v^{(j)}(i)|^{\frac{1}{2^j}} \right) \left| v^{(k)}(i) - b \right|^{\frac{1}{2^k}} < \log \alpha + \epsilon.$$

□

We immediately get the corollary

Corollary 7.2.3. *$\mathscr{S}_{[0,1]}$ is dense in (l,∞), for l defined in Lemma 7.2.7.*

An important detail omitted in the arguments here is the fact that, for odd b, $g_k^{(b)}(x)$ (and hence $r_k^{(b)}(x)$) is indeed irreducible. A proof is provided in Appendix B.1.

7.2.4 Generalisation to intervals with rational endpoints

The results derived for $[0,1]$ in the previous sections can be extended to a larger class of intervals. Recall that we obtained the Gorškov polynomials for $[0,1]$ by applying the transformation $\tau(x) = \frac{1}{1+x}$ to the roots. Now, take a pair of rationals $\frac{p}{q} < \frac{r}{s}$ with $sq > 0$ and construct the interval $\left[\frac{p}{q}, \frac{r}{s}\right]$. We may apply the Möbius transformation $\tau(x) = \frac{px+r}{qx+s}$ to the roots of $g_k(x)$ to obtain a new sequence of polynomials

$$R_k(x) = (qx-p)^{2^k} g_k\left(\frac{r-sx}{qx-p}\right), k \geq 0.$$

with leading coefficients

$$\begin{aligned}\lim_{x\to\infty} \frac{R_k(x)}{x^{2^k}} &= q^{2^k} g_k\left(-\frac{s}{q}\right) \\ &= q^{2^k} p_k\left(\sqrt{\frac{s}{q}}i\right) p_k\left(-\sqrt{\frac{s}{q}}i\right).\end{aligned}$$

As all the arguments from the previous section carry over to this case, we again get a sequence of polynomials with all roots in the interval, of degree 2^k, with relatively small leading coefficients. Again, the irreducibility of the $g_k(x)$ guarantees that the $R_k(x)$ are irreducible as well.

The normalised leading coefficients here tend to the limit

$$l_{q,s} = q \lim_{k\to\infty} \left(\prod_{j=1}^{k} \left| v^{(j)}\left(\sqrt{\frac{s}{q}}i\right)\right|^{\frac{1}{2^j}} \right) \left| v^{(k)}\left(\sqrt{\frac{s}{q}}i\right) - 1 \right|^{\frac{1}{2^k}}. \tag{7.31}$$

If we now use the $g_k^{(b)}(x)$ to construct a sequence $R_k^{(b)}(x)$ of generalised Gorškov polynomials for the interval, all the arguments from the previous section again carry over to prove the following:

Lemma 7.2.9. *Let* $I = \left[\frac{p}{q}, \frac{r}{s}\right]$ *with* $s, q > 0$. *Then the spectrum* S_I *is dense in* $(l_{q,s}, \infty)$, *where* $l_{q,s}$ *is as in (7.31).*

An alternative expression of this limit can be found in [16].

The important thing to note here is that, while this is a result for general intervals with rational endpoints, $l_{q,s}$ only depends on the denominators of the rationals. Thus, the result is only useful for those intervals which, among all intervals with endpoints of fixed denominators q, s, have the smallest length. These are the so-called Farey intervals – intervals whose endpoints are consecutive elements in a sequence of Farey fractions. Letting $S_0 = \{0, 1\}$, the k^{th} sequence S_k of Farey fractions is obtained by taking consecutive elements $\frac{p_j}{q_j}, \frac{p_{j+1}}{q_{j+1}}$ of the previous sequence S_{k-1} and inserting the rational $\frac{p_j+p_{j+1}}{q_j+q_{j+1}}$ between them. These sequences are best visualised by writing them in a tabular form, with S_{k-1} in the k^{th} row.

$$\begin{array}{ccccccccc}
\frac{0}{1} & & & & & & & & \frac{1}{1} \\
\frac{0}{1} & & & & \frac{1}{2} & & & & \frac{1}{1} \\
\frac{0}{1} & & \frac{1}{3} & & \frac{1}{2} & & \frac{2}{3} & & \frac{1}{1} \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots
\end{array}$$

Consecutive elements $\frac{p_j}{q_j}, \frac{p_{j+1}}{q_{j+1}}$ of S_k satisfy $\frac{p_{j+1}}{q_{j+1}} - \frac{p_j}{q_j} = \frac{1}{q_j q_{j+1}}$, as can be easily shown by induction. Thus, intervals with consecutive elements of S_k as endpoints have, among all intervals with endpoints rational endpoints of denominators q_j, q_{j+1}, the smallest length.

Chapter 8

Integer Transfinite Diameter and Critical Polynomials

8.1 The Integer Transfinite Diameter

In the introduction, we defined the transfinite diameter of a closed interval I of finite length on the real line by

$$t(I) = \lim_{n\to\infty} \inf_{p_n \in \mathbb{C}^*[x]} \|p_n\|_I^{\frac{1}{n}},$$

showing that its value, attained by the Chebyshev polynomials on I, is simply $\frac{|I|}{4}$. We then proceeded to restrict the set the infimum is taken over to polynomials with integer coefficients, while removing the restriction that the polynomials be monic, to get the so-called *integer transfinite diameter* or *integer Chebyshev constant*,

$$t_{\mathbb{Z}}(I) = \lim_{n\to\infty} \inf_{0\not\equiv p_n \in \mathbb{Z}_n[x]} \|p_n\|_I^{\frac{1}{n}}. \tag{8.1}$$

While the exact value of $t_{\mathbb{Z}}(I)$ is not known for any interval with $0 < |I| < 4$, Hilbert [29] showed that for these intervals,

$$\frac{|I|}{4} \le t_{\mathbb{Z}}(I) \le \sqrt{\frac{|I|}{4}}. \tag{8.2}$$

The following Lemma relates this quantity to our previous analysis of $\mathscr{S}_I$.

Lemma 8.1.1. *Let $q(x) = a_d x^d + \ldots + a_0 \in \mathbb{Z}_d(I)$ with $a_d > 0$. If $p_n(x) \in \mathbb{Z}_n[x]$ satisfies*

$$\|p_n\|_I^{\frac{1}{n}} < a_d^{-\frac{1}{d}}$$

then $q(x) \mid p_n(x)$.

Proof. We will prove the contrapositive. Assume p, q are as in the statement of the lemma and $\gcd(p,q) = 1$, let $\alpha_1, \ldots, \alpha_d$ denote the roots of q. Then the resultant of p_n and q satisfies

$$\left|\mathrm{Res}_x(p,q)\right| = a_d^n \prod_{i=1}^{d} |p(\alpha_i)|,$$

and is an integer (see discussion in Part I, Section 2.1). As this integer is further nonzero, we get

$$a_d^{-n} \leq \prod_{i=1}^{d} |p(\alpha_i)| \leq \|p\|_I^d,$$

and the result follows. □

The above Lemma plays a central role in the computation of lower and upper bounds for the integer transfinite diameter. We will look at these in turn.

8.2 Lower Bounds on $t_{\mathbb{Z}}(I)$

8.2.1 The classical lower bound

Let $I \subset \mathbb{R}$ be an interval with $0 < |I| < 4$ and consider a sequence of integer polynomials $\{g_k\}$, such that, for every $k \in \mathbb{N}$,

- $g_k \in \mathbb{Z}_{d_k}(I)$ is irreducible over $\mathbb{Q}$ with leading coefficient a_{d_k}
- $\gcd(g_k, g_i) = 1$ whenever $k \neq i$

Consider now some $P \in \mathbb{Z}[x]$. Clearly, only a finite number of g_k can divide P, so that

$$\limsup_{k\to\infty} a_{d_k}^{-\frac{1}{d_k}} \leq \|P\|_I^{\frac{1}{\partial P}},$$

by Lemma 8.1.1. Taking the infimum over all $P \in \mathbb{Z}[x]$, we get

$$\limsup_{k\to\infty} a_{d_k}^{-\frac{1}{d_k}} \leq t_{\mathbb{Z}}(I). \tag{8.3}$$

For $I = [0,1]$, we know one such sequence: the Gorškov polynomials for $[0,1]$ introduced in section 7.2 satisfy the conditions above (as was proved in the previous chapter), giving the classical lower bound

$$0.4207\ldots \leq t_{\mathbb{Z}}([0,1]). \tag{8.4}$$

Similarily, the generalisation of the Gorškhov polynomials to the Farey interval $I = \left[\frac{p}{q}, \frac{r}{s}\right]$ used in the previous section yield the lower bound

$$t_{\mathbb{Z}}\left(\left[\frac{p}{q}, \frac{r}{s}\right]\right) \geq \frac{1}{q+s} \prod_{i=0}^{\infty} (1+\lambda_i)^{-\frac{1}{2^{i+1}}} \tag{8.5}$$

where

$$\lambda_0 = \frac{qs}{(q+s)^2}, \lambda_{i+1} = \frac{\lambda_i}{(1+\lambda_i)^2}.$$

This is simply a different expression for (7.31), derived in [16].

It would be tempting to think that the lower bound produced by the Gorškov polynomials is best possible. In [9], Borwein and Erdélyi proved a striking result: using results by Saff and Varga in [41], together with the structure of the integer Chebyshev polynomials on $[0,1]$, they were able to show that, if, for fixed $\theta \in (0,1)$, the elements of a sequence of polynomials eventually have $\eta(\theta) d_k$ zeros in $\left[0, \theta^2\right)$ for some $\eta(\theta) \in (0,1)$, then

$$\gamma^{-1} \alpha^{-\eta(\theta)} \leq t_{\mathbb{Z}}([0,1]),$$

where $\gamma = \lim_{k\to\infty} |a_{d_k}|^{1/d_k}$ is the limit of the normalised leading coefficients of the polynomials and $\alpha \in (0,1)$ is a constant. This result easily generalises to real intervals with at least one rational endpoint. It follows that no real improvement on the lower

bound for $t_{\mathbb{Z}}(I)$ can be made by considering sequences of polynomials of this form for these intervals. Also, while $\eta(\theta), \alpha$ can be explicity computed for given $\theta > 0$, this does not improve the lower bound significantly, as $\eta(\theta)$ is too small.

In [38], Pritsker improved the lower bound, using weighted potential theory, to 0.4213, with room for improvement. His result makes use of the structure of P_n, the n^{th} integer Chebyshev polynomial.

8.2.2 Generalisation of the Gorškov polynomials

In an unpublished paper [25], Hare developed a method defining generalised sequences of Gorškov polynomials, producing lower bounds on $t_{\mathbb{Z}}(I)$. While his results do not improve the lower bound produced by the original polynomials for $I = [0,1]$, his methods can be used for any interval with rational endpoints and are thus of importance. The following results follow arguments in [25], and are reproduced here for completeness.

Hare's analysis relies on a generalisation of the classical Gorškov polynomials for $[0,1]$ by replacing the rational map

$$u(x) = \frac{x(1-x)}{1-3x(1-x)},$$

used to recursively define the $r_k(x)$ in (7.23) by a more general rational function: $u(x)$ is taken to be a rational function of the form $\frac{a(x)}{b(x)}$ with $\partial a = \partial b = 2$, mapping the interval $[0,1]$ onto itself twice.

Let $\mathbb{Q}(x)$ denote the field of rational functions over $\mathbb{Q}$. We also make the following definition:

Definition 8.2.1. Let $u(x) \in \mathbb{Q}(x), d \in \mathbb{N}$. We say that u maps the interval $[a,b]$ *d-fold* onto itself if the pre-image $u^{-1}([a,b]) = \{x \in \mathbb{C} : u(x) \in [a,b]\}$ satisfies the following:

- $u^{-1}([a,b]) \subset [a,b]$
- counting solutions according to their multiplicity, $\#\left(u^{-1}([a,b])\right) = d$.

A natural generalisation of the Gorškov polynomials can be achieved by considering

the set

$$\mathscr{U}_d[a,b] = \left\{u(x) \in \mathbb{Q}(x) : u(x) : [a,b] \mapsto [a,b] \text{ onto}, d-\text{fold}\right\}. \tag{8.6}$$

As it turns out, $\mathscr{U}_d[a,b]$ is easily described in terms of the explicit structure of the rational functions. We define the *content* of a polynomial to be the greatest common divisor of its coefficients.

Lemma 8.2.1. *Let $a,b \in \mathbb{Q}, b > a$. Every $u \in \mathscr{U}_d([a,b])$ is of the form*

$$u(x) = \frac{a \cdot e \cdot p(x) + b \cdot f \cdot q(x)}{e \cdot p(x) + f \cdot q(x)} \tag{8.7}$$

where $e, f \in \mathbb{Z}$, and $p(x), q(x) \in \mathbb{Z}_d(I)$ have content 1 and satisfy the following:

- $p(x)q(x) = (b_1 - b_2 x)(a_2 x - a_1) r(x)^2$, $r(x) \in \mathbb{Z}_{2d-2}[x]$
- *The roots $\alpha_1, \ldots, \alpha_d$ of $p(x)$ and $\beta_1, \ldots, \beta_d$ of $q(x)$ interlace.*

Proof. Considering the possible values of $u(x)$ at the endpoints, we see that there are four possible choices:

- $u(a) = u(b) = a$
- $u(a) = u(b) = b$
- $u(a) = a, u(b) = b$
- $u(a) = b, u(b) = a$.

A little thought shows that the first two occur in the case where d is even, whereas the last two occur for odd d. Also, the first two cases are related by the symmetry $x \mapsto (a+b) - x$, and the same holds for the last two. We will only consider the first case here, noting that the remaining three are handled similarly.

Consider $\text{numer}(u(x) - a)$. It follows from the properties of $u(x)$ that this is a polynomial with integer coefficients, with all d roots in $[a,b]$. Also, since $u(a) = u(b) = a$, two of these roots lie at the endpoints. Further, the polynomial has a root

of multiplicity two at the remaining roots $\alpha_1, \ldots, \alpha_{\frac{d}{2}-1} \in (a,b)$, as otherwise, there would exist some $x \in [a,b]$ with $u(x) < a$. Thus,

$$\begin{aligned}\operatorname{numer}(u(x)-a) &= \lambda(x-a)(b-x)\prod_{i=1}^{\frac{d}{2}-1}(x-\alpha_i)^2 \\ &= \lambda' \cdot p(x),\end{aligned}$$

where $p(x) = a_d x^d + \ldots + a_0 \in \mathbb{Z}_d[x]$ is a polynomial with $\gcd(a_0, \ldots, a_d) = 1$, and $\lambda' \in \mathbb{Z}$ is chosen arbitrary.

By a similar argument, we can show that

$$\operatorname{numer}(b-u(x)) = \mu' \cdot q(x),$$

where $q(x) \in \mathbb{Z}_d[x]$ is a polynomial with coprime coefficients, and μ' and arbitrary integer. Let now $s(x)$ be the least common denominator of $u(x)-a$ and $b-u(x)$. We then get the equations

$$\begin{aligned}u(x) - a &= \frac{e \cdot p(x)}{s(x)} \\ b - u(x) &= \frac{f \cdot q(x)}{s(x)},\end{aligned}$$

where e, f are integers obtained from λ', μ' after bringing the expressions on a common denominator. Adding these equations shows that

$$(b-a)s(x) = e \cdot p(x) + f \cdot q(x),$$

so that

$$\begin{aligned}u(x) &= \frac{e \cdot p(x)}{s(x)} + a \\ &= \frac{b \cdot e \cdot p(x) + a \cdot f \cdot q(x)}{e \cdot p(x) + f \cdot q(x)}.\end{aligned}$$

□

From the proof, it is apparent that, given $p(x)$ and $q(x)$ that satisfy the conditions

of the lemma, there is an infinite collection of $u(x)$, depending on the parameters $e, f \in \mathbb{Z}$. Clearly, we are interested in those $u(x) \in \mathscr{U}([a,b])$ that, for given $p(x) \in \mathbb{Z}[x]$, minimise the leading coefficient of $p(u(x))$.

Given a polynomial $g(x) = g_0 + \ldots + g_d x^d \in \mathbb{Z}_d[x]$ and a rational function $u(x) = \frac{a(x)}{b(x)}$, we have

$$\operatorname{numer}(g(u(x))) = \sum_{i=0}^{d} g_i a(x)^i b(x)^{n-i}.$$

Thus, if we want to keep the leading coefficient of $g(x)$ small, we need to choose $a(x)$ and $b(x)$ with small leading coefficients. We thus want to choose e, f in a way to minimize the size of the coefficients of both $a(x)$ and $b(x)$. Setting $a = \frac{a_1}{a_2}, b = \frac{b_1}{b_2}$ and bringing (8.7) on a common denominator, we get

$$\frac{a_1 \cdot b_2 \cdot e \cdot p(x) + b_1 \cdot a_2 \cdot q(x)}{a_2 \cdot b_2 \cdot (e \cdot p(x) + f \cdot q(x))}.$$

Here, the leading coefficients of both top and bottom are minimised when setting $e = a_2, f = b_2$, which turns (8.7) into

$$u(x) = \frac{a_1 \cdot p(x) + b_1 \cdot q(x)}{a_2 \cdot p(x) + b_2 \cdot q(x)}. \tag{8.8}$$

This agrees with Flammang's generalisation of the Gorškov polynomials for $\left[\frac{a_1}{a_2}, \frac{b_1}{b_2}\right]$: Under the transformation $\tau(x) = \frac{b_1 + a_1 x}{b_2 + a_2 x}$, the Gorškov polynomials for $[0,\infty)$, defined in (7.16), turn into $P_k(x)$ satisfying

$$\begin{aligned} P_0(x) &= a_2 x - a_1 \\ P_k(x) &= \operatorname{numer}(P_{k-1}(u(x)), k \geq 1, \\ u(x) &= \frac{b_1(a_1 x - a_2)(b_2 - b_1 x) + a_1[(a_1 + b_1) - (a_2 + b_2)x]^2}{b_2(a_1 x - a_2)(b_2 - b_1 x) + a_2[(a_1 + b_1) - (a_2 + b_2)x]^2}. \end{aligned}$$

This is simply the rational function obtained through Hare's method, using the three linear polynomials with roots in the interval and small leading coefficients.

Hare also makes use of two simple lemmas. Set $\mathscr{U}[a,b] = \bigcup_{d=1}^{\infty} \mathscr{U}_d[a,b]$.

Lemma 8.2.2. *Let $p(x)$ have all roots in $I = [a,b]$, $u(x) \in \mathscr{U}[a,b]$. Then* $\operatorname{numer}(p(u(x)))$

has all roots in I.

Lemma 8.2.3. *Let $u(x) \in \mathscr{U}[a,b]$. Then all real roots of* $\mathrm{numer}(u(x)-x)$ *lie in $I = [a,b]$.*

Using these lemmas, he systematically searches for sequences of generalised Gorškov polynomials for $I = \left[\frac{a_1}{a_2}, \frac{b_1}{b_2}\right]$, as follows:

1. Start with $\mathscr{Q} = \{a_1 - a_2 x, b_1 - b_2 x, (a_1+b_1) - (a_2+b_2)x\}$.

2. From $\mathscr{Q}$, construct the set $\mathscr{P}$ of all pairs of polynomials satisfying the conditions of Lemma 8.2.1.

3. Using rational functions $u(x) \in \mathscr{U}[a,b]$ constructed from $\mathscr{P}$ together with Lemmas 8.2.2 and 8.2.3, extend $\mathscr{Q}$.

4. Repeat steps 2 and 3 until some criteria are met – for example, the maximal degree of the polynomials exceeds some bound $N \in \mathbb{N}$. At this point, use $\mathscr{Q}$ and rational functions constructed from $\mathscr{P}$ to construct sequences of polynomials with all their roots in I, giving lower bounds on $t_{\mathbb{Z}}(I)$.

As mentioned before, this method did not produce any improved lower bounds for $t_{\mathbb{Z}}([0,1])$. Its strength lies in the fact that it allows computation of lower bounds on the integer transfinite diameter for any interval with rational endpoints, and not just Farey intervals. A list of lower bounds for a variety of intervals can be found in the paper.

8.3 Upper bounds and Critical Polynomials

The classical method of obtaining upper bounds on $t_{\mathbb{Z}}(I)$ is through explicit computation of small polynomials on I. We therefore start our discussion here.

For some $I \subset \mathbb{R}$, $n \in \mathbb{N}$, let $P_n \in \mathbb{Z}_n[x]$ have the property that

$$\|P_n\|_I^{\frac{1}{\partial P_n}} = \inf_{p_n \in \mathbb{Z}_n[x]} \|p_n\|_I^{\frac{1}{\partial p_n}},$$

so $P_n(x)$ is the n^{th} integer Chebyshev polynomial. This polynomial is not always unique, as Montgomery's computations for $n = 2,3,\ldots$ in [35] show. It is actually an open question, posed by Borwein and Erdélyi in [9], whether there exists some sufficiently large $N \in \mathbb{N}$ such that, for $n > N$, P_n is indeed unique. We will first examine the structure of P_n for large n.

8.3.1 Structure of P_n, $n \to \infty$

While Lemma 8.1.1 plays an important role in finding lower bounds on the integer transfinite diameter, it also tells us a lot about the structure of P_n, $n \in \mathbb{N}$: in contrast to the classical Chebyshev polynomials defined in (6.1), P_n will have a number of factors of high multiplicities, as any polynomial $q(x) = a_d x^d + \ldots + a_0 \in \mathbb{Z}_n[x]$ with all roots in I and $|a_d|^{-\frac{1}{d}} < \|P_n\|_I^{\frac{1}{\partial P_n}}$ has to be a factor of P_n. Letting $n \to \infty$, we make the following definition, following [20]:

Definition 8.3.1 (Critical Polynomial)**.** Let $q(x) = a_d x^d + \ldots + a_0 \in \mathbb{Z}_n[x]$ with $a_d > 1$. If $a_d^{-\frac{1}{d}} > t_{\mathbb{Z}}(I)$, q is said to be **critical** for I.

This definition of course assumes that the actual value of $t_{\mathbb{Z}}(I)$ is known – unfortunately, this is usually not the case. Thus, to prove that a polynomial $q(x) = a_d x^d + \cdots$ is critical, one generally has to explicitly find a polynomial $p(x)$ with $a_d^{-\frac{1}{d}} > \|p\|_I^{\frac{1}{\partial p}}$, from which $a_d^{-\frac{1}{d}} > t_{\mathbb{Z}}(I)$ follows.

Returning now to the problem of determining the polynomial P_n, let us consider $I = [0,1]$. For the first few values of n, we get the following polynomials (taken from [35]):

n	Polynomial	$\|P_n\|_{[0,1]}^{\frac{1}{n}}$
1	$x, 1-x, 1-2x$	1
2	$x(1-x)$	$\frac{1}{2}$
3	$x(1-x)(1-2x)$	$\frac{1}{2.18\ldots}$
4	$x^2(1-x)^2, x(1-x)(1-2x)^2$	$\frac{1}{2}$

A few natural questions, aside from uniqueness of P_n, arise at this point:

1. For $n \in \mathbb{N}$, does there always exists a P_n such that the factors x and $(1-x)$ occur

to the same multiplicity?

2. Like the (non-integral) Chebyshev polynomials, do integer Chebyshev polynomials have all their roots in the interval? In other words, is the converse of Lemma 8.1.1 true?

3. Does each critical polynomial eventually occur of arbitrarily high multiplicity in the factorisation of P_n as $n \to \infty$?

4. Is $\lim_{n\to\infty} P_n$ even a polynomial, or does it have infinitely many distinct factors? If it has infinitely many factors, what proportion of them are critical polynomials?

The first question is answered by a simple corollary of a theorem due to Amoroso in [6]:

Proposition 8.3.1. *Let $P \in \mathbb{Z}_d[x]$ be a polynomial of degree d with leading coefficient b_d and let $X \subset \mathbb{C}$ be compact. Then*

$$\frac{1}{|b_d|} t_{\mathbb{Z}}(X) \leq t_{\mathbb{Z}}\left(P^{-1}(X)\right)^d \leq t_{\mathbb{Z}}(X).$$

Proof. For the first inequality, suppose $p_n \in \mathbb{Z}_n[x]$ and let $R(x) = \mathrm{Res}_t(p_n(t), x - P(t)) \in \mathbb{Z}[x]$. Note that this resultant takes the form

$$b_d^n \prod_{i=1}^{d} p_n(t_i),$$

where the product is taken the d solutions $t_1, \ldots, t_d$ of $P(t_i) = x$. Note that $\partial_x(R) = n$, since $\mathrm{Res}_x(f, g)$ is a polynomial of degree $\partial_x f$ in the coefficients of $g(x)$ (see Part I, Theorem 2.1.1). Thus,

$$\begin{aligned} t_{\mathbb{Z}}(X) &\leq \|R\|_I^{\frac{1}{n}} \\ &\leq |b_d| \prod_{i=1}^{d} \|p_n\|_{P^{-1}(X)}^{\frac{1}{n}} \\ &= |b_d| \, \|p_n\|_{P^{-1}(X)}^{\frac{d}{n}}. \end{aligned}$$

Taking now the $\liminf_{n\to\infty}$ on the right-hand side gives the first inequality.

For the second inequality, note that, for any $p_n \in \mathbb{Z}_n[x]$,

$$\|p_n\|_X = \|p_n \circ P\|_{P^{-1}(X)}.$$

We get

$$\begin{aligned} t_{\mathbb{Z}}(P^{-1}(X)) &\leq \inf_{0 \neq p_n \in \mathbb{Z}_n[x]} \|p_n\|_{P^{-1}(X)}^{\frac{1}{n}} \\ &\leq \|p_n \circ P\|_X^{\frac{1}{dn}} = \left(\|p_n\|_X^{\frac{1}{n}}\right)^{\frac{1}{d}}. \end{aligned}$$

The result now follows, once again, by taking the $\liminf_{n\to\infty}$ of the right hand side. □

Using this result together with the map

$$\begin{aligned} P : [0,1] &\to \left[0, \tfrac{1}{4}\right] \\ x &\mapsto x(1-x) \end{aligned}$$

we see that the integer transfinite diameters of $[0,1]$ and $\left[0, \frac{1}{4}\right]$ are directly related by

$$t_{\mathbb{Z}}([0,1]) = t_{\mathbb{Z}}\left(\left[0, \tfrac{1}{4}\right]\right)^2.$$

This shows that some integer Chebyshev polynomial for $[0,1]$ must always be a polynomial in $x(1-x)$, therefore showing that the exponents of x and $1-x$ are equal.

The second question, conjectured by the authors in [9], was settled soon after the original paper, by Habsieger and Salvy. In their paper [24], they compute P_{70} to be

$$\begin{aligned} P_{70}(x) = &x^{22}(1-x)^{22}(1-2x)^8(1-5x+5x^2)^2(29x^4-58x^3+40x^2-11x+1) \\ &(4921x^{10}-24605x^9+53804x^8-67586x^7+53866x^6-28388x^5+9995x^4 \\ &-2317x^3+338x^2-28x+1). \end{aligned}$$

What makes this polynomial interesting is the occurrence of the degree 10 factor, which has 4 nonreal roots, disproving the conjecture and showing that, unlike the classical Chebyshev polynomials, integer Chebyshev polynomials can have roots outside of the interval in question. Since Habsieger and Salvy discovered this factor

in their paper, more factors of integer Chebyshev polynomials with complex roots have been found, most recently by Flammang in [17].

To answer the third question, one employs Markov's Inequality for polynomials (see [8] for example). Let $p_n \in \mathbb{Z}_n[x]$ be a polynomial of degree n and p_n' its derivative. Then

$$\|p_n'\|_{[a,b]} \leq \frac{b-a}{2} n^2 \|p_n\|_{[a,b]} . \tag{8.9}$$

Taking n^{th} roots of both sides and noting that

$$\lim_{n\to\infty} \left(\frac{b-a}{2} n^2\right)^{\frac{1}{n}} = 1,$$

we see that, for n sufficiently large, a critical polynomial has to also be a factor of the derivative of the n^{th} integer Chebyshev polynomial. Repeated application of Markov's inequality extends this to derivatives of arbitrary order, so that critical polynomials eventually occur as factors of arbitrarily high multiplicity in the factorisation of integer Chebyshev polynomials.

The final question about the structure of integer Chebyshev polynomials was answered by Pritsker in [38]. He showed that the limiting function $\lim_{n\to\infty} P_n$ is not actually a polynomial, but must consist of infinitely many factors (Theorem 1.8 in his paper). This, in connection with the following theorem due to Hare and Smyth in [27], provides some hope that there might exist an explicit expression for $t_{\mathbb{Z}}(I)$, at least for some I:

Proposition 8.3.2 (Hare & Smyth 2005)**.** *Let $I \subset \mathbb{R}$ and $\{q_k\}_{k=1}^{\infty}$ be a sequence of distinct critical polynomials with $\partial q_k = d_k$ and leading coefficients $a_{d_k} > 1$. Then*

$$\inf_k a_{d_k}^{-\frac{1}{d_k}} = t_{\mathbb{Z}}(I).$$

Unfortunately, not a single such I is known. Even worse, it is not even known whether every real interval has at least one critical polynomial. The only partial result in this area is due to Hare and Smyth in the same paper, where they show that every interval not containing an integer in its interior has a linear critical polynomial. A

proof of this can be found in section 9.2.

A lot more is known about the structure of n^{th} integer Chebyshev polynomial, especially for $I = [0,1]$. Using orthogonal Müntz-Legendre polynomials on $[0,1]$ (see [8] for details on these polynomials), Borwein and Erdélyi showed the following in [9]:

Proposition 8.3.3. *As $n \to \infty$, the n^{th} integer Chebyshev polynomial P_n for $[0,1]$ takes the form*

$$P_n(x) = x^k(1-x)^k R_{n-2k}(x)$$

where $k > 0.26n$ and $R_{n-2k} \in \mathbb{Z}_{n-2k}[x]$.

Similar results can be obtained using the same techniques for arbitrary intervals with rational endpoints. This result shows that the integer Chebyshev polynomials, when normalised by their degree, behave rather like "weighted polynomials" – a result Pritsker used in his 2005 paper [38], with the help of weighted potential theory, to improve both lower and upper bounds on $t_{\mathbb{Z}}([0,1])$. He also improved the bounds for the weights to

$$0.31 \leq \frac{k_1}{n} \leq 0.34, \quad 0.11 \leq \frac{k_2}{n} \leq 0.14 \text{ and } 0.035 \leq \frac{k_3}{n} \leq 0.057$$

where

$$P_n(x) = (x(1-x))^{k_1}(1-2x)^{k_2}(5x^2-5x+1)^{k_3} R_{n-2k_1-k_2-2k_3} \text{ for } n \to \infty.$$

All these results were obtained for $\left[0, \frac{1}{4}\right]$, and then mapped to $[0,1]$ using $x \mapsto x(1-x)$. Generally, when computing results for $[0,1]$, it is more efficient to work on $\left[0, \frac{1}{4}\right]$, as this halves the degree of all polynomials involved.

From this discussion, especially with regard to the asymptotic structure of P_n, it is clear that critical polynomials play a pivotal role in the theory of the integer transfinite diameter, and having methods to find critical polynomials is of some importance.

8.3.2 Computational methods for finding small polynomials

Algorithms to search for polynomials with small supremum norm on an interval I can be split into various categories:

1. Algorithms based on a method developed by Habsieger and Salvy,
2. algorithms based on LLL, and
3. algorithms based on a generalisation of the Gorškov polynomials.

The first class of algorithms are based on the work of Habsieger and Salvy in their 1997 paper [24]. There, they computed the integer Chebyshev polynomials for $[0,1]$ up to degree 75. To do this, they used a recursive algorithm. Assuming one has calculated the k^{th} integer Chebyshev polynomials for $1 \leq k < n$ and wants to find the n^{th} integer Chebyshev polynomial, they proceed as follows:

- Find an upper bound for $\|P\|_I$. They use $\max_{1<p<n} \|P_p P_{k-p}\|_I = c_n$.
- Given this bound and a list of known factors, check which factors have to divide P. Use Markov's inequality to gain information on the exponents of the factors.
- If this does not produce a polynomial of degree n, use integer linear programming on a set of control points in I to explicitly calculate the coefficients of the missing polynomial. This last step is the bottleneck of the algorithm.

It is of course the last step in this algorithm that can be used to find new critical polynomials. The problem is that the crucial step here is computationally very expensive. In their computations of critical polynomials up to degree 75, Habsieger and Salvy came across no previously unknown critical polynomials, but found the degree 10 factor with four nonreal roots mentioned earlier.

Subsequently, the methods employed by Habsieger and Salvy were improved by Wu [45] and recently used by Flammang [17] to find a list of critical polynomials. They use a combination of Habsieger and Salvy's method with the LLL algorithm to find a list of factors of degree up to 8 for $I = \left[0, \frac{1}{4}\right]$.

The Lenstra, Lenstra, and Lovasz (LLL) basis reduction algorithm [32] is a modification of the well-known Gram-Schmidt orthogonalisation process, applied to a lattice.

Given a lattice Λ with a basis B, LLL produces a new basis B' for Λ, where the elements of B' are "small" with respect to a given norm.

There are various ways in which this can be applied to the problem of finding small polynomials with integer coefficients. Wu and Flammang use a set of control points $X \subset I$ and then apply LLL with the usual Euclidean Norm to the basis $B = \{f(x), f(x)x, f(x)x^2, \ldots, f(x)x^{n-k}\}_{x\in X}$ for a $\mathbb{R}$-lattice Λ, where $f(x) \in \mathbb{Z}_k[x]$ is a known small polynomial for I. Based on the reduced basis B', they then obtain a polynomial of degree n with small supremum norm on the interval.

One can also use the lattice structure of $\mathbb{Z}_n[x]$ over $\mathbb{R}[x]$ directly, with the inner product $\langle f, g\rangle = \frac{1}{b-a}\int_a^b f(x)g(x)dx$, or a discrete version $\langle f, g\rangle = \frac{1}{|X|}\sum_{x\in X} f(x)g(x)$ for a finite $X \subset I$.

Finally, one can use Hare's generalisation of the Gorškov polynomials outlined in the previous section. As can be seen from the example of the classical Gorškov polynomials, the first few elements in the sequence $\{r_k(x)\}$ are critical polynomials. This naturally leads to a search for critical polynomials as elements of sequences of generalised Gorškov polynomials.

Using a combination of the methods outlined here, Kevin Hare [26] has produced a list of over 200 polynomials with all roots in $[0,1]$ and normalised leading coefficients $a_d^{\frac{1}{d}} < 2.3768$. The interested reader is encouraged to contact him directly about this list.

To determine which of these polynomials is actually critical of course requires the computation of a small polynomial on $[0,1]$.

8.4 Isolated points of $\mathscr{S}_I$

Using the methods of the previous section, we can find a list of possible factors of integer Chebyshev polynomials for a given interval $I \subset \mathbb{R}$. We will now turn to methods to use this list to find a discrete subset of $\mathscr{S}_{[0,1]}$ and, at the same time, improve the known upper bound for $t_{\mathbb{Z}}([0,1])$.

8.4.1 Explicitly finding small polynomials

Suppose we are given a list of polynomials $L = \{p_i\}_{i=1}^{N}$ with integer coefficients. Using Lemma 8.1.1, we may want to use these polynomials as factors of some $P \in \mathbb{Z}[x]$ with $\|P\|_I^{\frac{1}{\partial P}} = m$ as small as possible. As all $q_i(x) = a_{d_i,i}x^{d_i} + \ldots + a_{0,i} \in L$ with $_{d_i,i} > 0$ and all roots in I and $a_{d_i,i}^{-\frac{1}{d_i}} > \|P\|_I^{\frac{1}{\partial P}}$ have to be factors of P, we know that L then contains a complete list of polynomials with all roots in I and $a_d^{-\frac{1}{d}} > m$.

How do we find this P? The natural approach is to consider the function

$$F(x) = \prod_{i=1}^{N} |p_i(x)|^{\frac{c_i}{\partial p_i}}$$

with $\sum_{i=1}^{N} c_i = 1$, and attempt to find $\boldsymbol{c} = (c_1, \ldots, c_N)$ to minimise the maximum of $F(x)$ on I. This problem is easily solved by considering the logarithm and turning it into a discrete optimisation problem, by solving it over a suitable finite subset $X \subset I$.

More specifically, if we let

$$f(x, \boldsymbol{c}) = \sum_{i=1}^{N} \frac{c_i}{\partial p_i} \log|p_i(x)|, \tag{8.10}$$

and choose some finite $X \in I$, we can use linear programming methods to solve the optimisation problem

$$\begin{cases} \min & m \\ \text{s.t.} & f(x, \boldsymbol{c}) \leq m \\ & \sum_{i=1}^{N} c_i = 1 \\ & c_i \geq 0 \\ & x \in X. \end{cases} \tag{8.11}$$

Then the resulting function $F(x)$ will have small $\|F\|_I$. By taking a sufficiently high power of $F(x)$, we can then recover the polynomial $P(x)$ (of generally quite large degree).

8.4.2 Auxiliary functions

An alternative method was developed by Smyth [43], for the analysis of the spectrum of the Mahler measure of totally real algebraic integers with roots on the positive real

line and later in[44] generalised.

Suppose we are given some mean of algebraic integers – an expression in the conjugates $\alpha^{(1)},\dots,\alpha^{(n)}$ of the algebraic integer α of degree n, for example

$$\begin{aligned} M(\alpha) &= \prod_{i=1}^{n} \max\left\{1,|\alpha^{(i)}|\right\} && \text{(Mahler measure)} \\ \Omega_p(\alpha) &= \left(\frac{1}{n}\sum_{i=1}^{n}|\alpha^{(i)}|^p\right)^{\frac{1}{p}} && (p\text{-th Mean Value}) \\ \mathrm{N}(\alpha) &= \left(\prod_{i=1}^{n}|\alpha^{(i)}|\right)^{\frac{1}{n}}. && \text{(normalised Norm)} \end{aligned}$$

Suppose we are given some list of algebraic integers $L=\{\alpha_1,\dots,\alpha_N\}$ with $\mathbb{Q}(\alpha_i)\cap\mathbb{Q}(\alpha_j)=\mathbb{Q}$ whenever $i\neq j$, small means $\Omega(\alpha_1),\dots,\Omega(\alpha_N)$, and with minimal polynomials $P_1,\dots,P_N$ over $\mathbb{Q}$. Further, we will assume $\Omega(\alpha)$ can be written as $\Omega_p(\alpha)=\frac{1}{n}\sum_{i=1}^{n}\omega\left(\alpha^{(i)}\right)$, a sum of expressions in the conjugates of α, such as $\log\mathrm{N}(\alpha)=\frac{1}{n}\sum_{i=1}^{n}\log\alpha^{(i)}$, or $\Omega_p(x)^p$ above. Clearly, for any $\alpha\notin L$ (meaning that $\mathbb{Q}(\alpha_i)\cap\mathbb{Q}(\alpha)=\mathbb{Q}$ for any $\alpha_i\in L$) of degree n and with conjugates $\alpha=\alpha^{(1)},\dots,\alpha^{(n)}$, the product

$$\prod_{i=1}^{n}\left|P_j(\alpha^{(i)})\right|$$

is a nonzero integer, for $1\le j\le N$. Thus,

$$\sum_{i=1}^{n}\log\left|P_j(\alpha^{(i)})\right|\ge 0, 1\le j\le N. \tag{8.12}$$

We now define a (real) measure μ_α on $[0,\infty)$ by

$$\mu_\alpha(x)=\tfrac{1}{n}\left(\#\text{ of conjugates of }\alpha\text{ in }(0,x]\right)$$

Using this, we may write (8.12) as

$$\int_0^\infty \log\left|P_j(x)\right| d\mu_\alpha(x)\ge 0.$$

Thus, we are faced with the following optimisation problem.

$$\begin{cases} \min_{\mu} & \int_0^\infty \omega(x)\, d\mu(x) \\ \text{s.t.} & \int_0^\infty \log\left|P_j(x)\right| d\mu(x) \geq 0, \quad j = 1,\ldots,N \end{cases}$$

While we certainly cannot solve this problem using linear programming, we can find an upper bound for the solution by approximating it by the solution of a discrete version of the problem. Let $X = \{x_1,\ldots,x_k\} \subset [0,\infty)$. Then we have

$$\begin{cases} \min & \sum_{i=1}^k \omega(x_i)\, t_i \\ \text{s.t.} & \sum_{i=1}^k \log\left|P_j(x_i)\right| t_i \geq 0, \quad j = 1,\ldots,n \\ & \sum_{i=1}^k t_i = 1 \\ & t_i \geq 0, \quad i = 1,\ldots,k \end{cases}$$

Instead of solving this problem directly, we will instead consider the dual: Let $\omega_i = \omega(x_i)$. The dual problem is then

$$\begin{cases} \max & m \\ \text{s.t.} & \omega_i - \sum_{j=1}^n c_j \log\left|P_j(x_i)\right| \geq m, \quad i = 1,\ldots,k \\ & c_j \geq 0, \quad j = 1,\ldots,n. \end{cases} \tag{8.13}$$

This version of the optimisation problem is often called the method of "auxiliary functions": we consider $g(x,\boldsymbol{c}) = \omega(x) - \sum_{j=1}^n c_j \log|p_j(x)|$ as an "auxiliary function" in solving the problem, as by (8.12), we have

$$\begin{aligned} \sum_{i=1}^d g(\alpha^{(i)},\boldsymbol{c}) &= \sum_{i=1}^d \omega(\alpha^{(i)}) - \sum_{i=1}^d \sum_{j=1}^n c_j \log\left|p_j\left(\alpha^{(i)}\right)\right| \\ &\geq \Omega(\alpha) \end{aligned}$$

Auxiliary functions of various types have been used by a number of authors to obtain results of this type for a variety of problems [43, 18, 3, 19], and more recently, [17].

For our setting – the spectrum $\mathscr{S}_{[0,1]}$ – note that, if α is an algebraic integer with all conjugates in $[1,\infty)$, then $\frac{1}{\alpha}$ is an algebraic number with all conjugates in $[0,1]$ and $a_n = \mathrm{N}(\alpha)$ (where a_n denotes the leading coefficient of the minimal polynomial

of $\frac{1}{\alpha}$). Thus, we will be using the measure $\Omega(x) = \log \mathrm{N}(x)$, which turns (8.13) into

$$\begin{cases} \max & m \\ \text{s.t.} & \log(x) - \sum_{j=1}^{n} \frac{c_j}{\partial P_j} \log\left|P_j(x_i)\right| \geq m, \quad i = 1, \ldots, N \\ & c_j \geq 0, \quad j = 1 \ldots n. \end{cases} \tag{8.14}$$

Note that we have changed the problem slightly, normalising each coefficient in the auxiliary function by the degree of its corresponding factor. Consider now the problem under the change of variable $x \mapsto \frac{1}{x}$. Now, the auxiliary function turns into

$$\begin{aligned} g(x, \boldsymbol{c}) &= -\log x - \sum_{j=1}^{n} \frac{c_j}{\partial P_j} \log\left|P_j\left(\frac{1}{x}\right)\right| \\ &= -\log x - \sum_{j=1}^{n} \frac{c_j}{\partial P_j} \log\left|\frac{1}{x^{\partial P_j}} P_j^*(x)\right| \\ &= \log x \left(\sum_{i=1}^{n} c_i - 1\right) - \sum_{j=1}^{n} \frac{c_j}{\partial P_j} \log\left|P_j^*(x)\right|, \end{aligned}$$

where $P_j^*(x) = x^{\partial P_j} P_j\left(\frac{1}{x}\right)$ is the reciprocal polynomial of $P_j(x)$. Setting now $m = -M$ and imposing the additional condition $\sum_{i=1}^{n} c_i = 1$, we get the same optimisation problem as in (8.11).

8.4.3 Semi-infinite linear programming

To solve the optimisation problem (8.11) (and thus the one in (8.14) with the added constraints), we use a method known as semi-infinite linear programming, successively approximating the solution of the actual (infinite) problem by the solution of a finite optimisation problem.

Let $f(x, \boldsymbol{c})$ be as in (8.10), $m_1 = 0$.

1. Let X_1 be a set of 50 evenly distributed sample points in $I = [0, 1]$.
2. Solve the problem on X_1, using the simplex method, obtaining $\boldsymbol{c}_1$ and $m_1 = \max_{x \in X_1} f(x, \boldsymbol{c}_1)$. Let $M_1 = \|f(x, \boldsymbol{c}_1)\|_I$. Clearly, $m_1 < M_1$.
3. Let E_1 be the set of extrema of $f(x, \boldsymbol{c}_1)$ in I. Set $X_2 = E_1 \cup X_1$.
4. Repeat step (2) for X_2, obtaining m_2 and M_2.

Repeating this algorithm, we get sequences $m_1 < m_2 < \ldots$ and $M_1 > M_2 > \ldots$ with $m_k < M_k$ for all $k \in \mathbb{N}$ and

$$\lim_{k\to\infty} m_k = \inf_{\boldsymbol{c}} \|f(x,\boldsymbol{c})\|_I = \lim_{k\to\infty} M_k.$$

Thus, for a given $\epsilon > 0$, we may find $K \in \mathbb{N}$ with

$$M_K - m_K < \epsilon,$$

so that we can approximate the solution of the actual problem to arbitrary precision this way.

To find the maxima of $f(x,\boldsymbol{c})$ to, we use the real roots of the function (which we can easily compute, as we have a complete factorisation of $\exp(f(x,\boldsymbol{c}))$ to find intervals isolating the extrema. In the case of complex roots, we use Jensen circles to gain information on the location of the minima:

If the polynomial $p(z)$ has a complex root at $z = z_0$, then the derivative has a root in the circle $|\Re(z_0) - z| < |\Im(z_0)|$ (the Jensen circle of $p(z)$ at z_0). Consider now a pair $z_0, \overline{z_0}$ of complex roots of the polynomial $p(z)$, and suppose (without loss of generality) that the extrema of $p(z)$ contained in the Jensen circle centred at $z = \Re(z_0)$ is a minimum. The value of $|p(z_0)|$ will then be smaller than $|p(z)|$ at the adjacent extrema, so that we do not have to consider this extrema as a possible maximum of $\log|p(z)|$ (see Figure 8.1 for an example). This leads to the following method for finding intervals containing the extrema of $p(z)$, using Jensen circles.

Let z_1, z_2 be two roots of the polynomial $p(z)$ with $|p(z)| < 1$ for $z \in I$.

- If $\Im(z_1) = \Im(z_2) = 0$, then $\log|p(z)|$ has a maximum in (z_1, z_2).
- If $\Im(z_1) \neq 0, \Im(z_2) = 0$, then $\log|p(z)|$ has a maximum in $(\Re(z_1) - |\Im(z_1)|, z_2)$
- If $\Im(z_1) = 0, \Im(z_2) \neq 0$, then $\log|p(z)|$ has a maximum in $(z_1, \Re(z_2) + |\Im(z_2)|)$
- If $\Im(z_1) \neq 0, \Im(z_2) \neq 0, \Re(z_1) \neq \Re(z_2)$, then $\log|p(z)$ has a maximum in $(\Re(z_1) - |\Im(z_1)|, \Re(z_2) + |\Im(z_2)|)$.

Using these intervals together with MATLAB's `fminbnd` function (an implementation

of Brent's method from [37]) allows us to efficiently find all extrema of $f(x,\boldsymbol{c})$ to high precision (10^{-14} in this case).

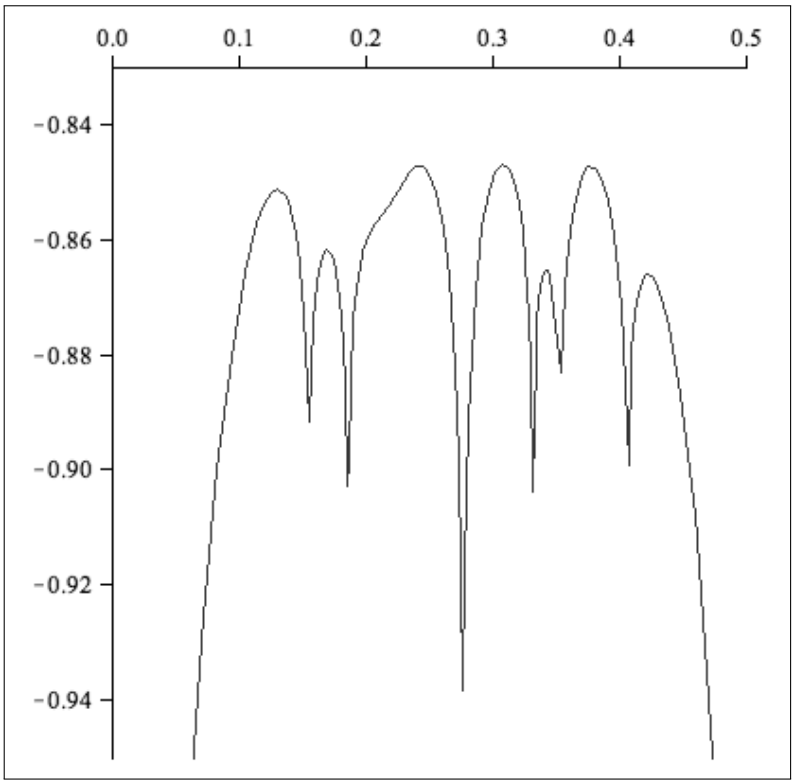

Figure 8.1: $f(x) = \frac{1}{70}\log|P_{70}(x)|$ of $P_{70}(x)$, the 70-th integer Chebyshev polynomial. Note that, while the polynomial has a pair of complex roots at $0.2164 \pm 0.0228i$, $f(x)$ only has one extremum between $x = 0.1855$ and $x = 0.2764$.

Using the list of polynomials found by Flammang [17], together with all polynomials in Hare's list [26] of degree up to 9, after a number of iterations, we get some $k \in \mathbb{N}$ with $M_k - m_k < 10^{-5}$ and $e^{M_k} \approx 0.42289421$, thus proving

1. There are only 6 isolated points of $\mathscr{S}_{[0,1]}$ in $[1, 2.3647]$.

2. $t_{\mathbb{Z}}([0,1]) \leq 0.42289421$.

The resulting polynomial can be found in Table 8.1. Polynomials marked with an asterisk $*$ are critical – they have the property that $p_i(x(1-x)) = a_{d_i}x^{d_i} + \ldots + a_0$ has $a_{d_i}^{\frac{1}{d_i}} < 2.3646$ and all roots in $[0,1]$. The F/H indicates whether the polynomial appeared in Flammang's paper (F), was found by Hare (H), or appeared in both (F/H).

The polynomial was obtained by starting with Flammang's list of factors and successively adding in elements from Hare's list, starting with the lowest-degree polynomials. If, after adding a factor, the semi-infinite linear programming routine produced an improved value for m, the additional factor was kept; otherwise it was discarded. In this case, computations were done in MATLAB, using double precision.

Interestingly, while we ran the computations far beyond degree 8 factors in Hare's list, additional higher-degree factors (aside from the factor of degree 9) did not lead to a further improvement. This, together with the structure of the final polynomial, suggests that non-critical polynomials – polynomials with nonreal roots, or with larger normalised leading coefficients – play an important role in the theory of the integer Chebyshev constant as well.

Any results for $[0,1]$ can easily be generalised to an arbitrary Farey interval: seeing that solving a direct optimisation problem is equivalent to solving a problem involving auxiliary functions for the normalised norm of algebraic integers on $[1,\infty)$, one can then use a linear fractional transformation to map the results for $[1,\infty)$ to the required Farey interval, as outlined in section 7.2.4. A detailed discussion of this can be found in the recent paper [4]. Note that our table contains one polynomial with constant coefficient 2, which has to be omitted, as its reciprocal is not an algebraic integer.

Table 8.1: The extremal polynomial $P(x)=\prod_{i=1}^{41} p_i(x(1-x))^{a_i}$. $\|P\|_{[0,1]}^{\frac{1}{\partial P}} \approx 0.42289421$

$p_i(x)$										a_i	
								1		629747702979896	$F/H*$
								4	−1	113679312593902	$F/H*$
								5	−1	75983357771784	$F/H*$
								6	−1	3571079405147	F
							29	−11	1	27919832711876	$F/H*$
							33	−12	1	1080201023794	F
							34	−12	1	432014474974	F
							49	−20	2	364480845799	F
						169	−94	17	−1	7412454948533	$F/H*$
						193	−104	18	−1	288134693918	F
						199	−105	18	−1	496982742428	F
					941	−703	193	−23	1	6481726119896	$F/H*$
					961	−712	194	−23	1	3593621901943	$F/H*$
				4921	−4594	1697	−310	28	−1	270204043363	F
				5501	−5075	1845	−330	29	−1	333759141598	F
				5601	−5140	1859	−331	29	−1	90982045747	H
			30689	−34148	15627	−3760	501	−35	1	512660676915	F
			31169	−34564	15761	−3779	502	−35	1	423481224544	F
			31269	−34629	15775	−3780	502	−35	1	193238390102	F
			32041	−35238	15951	−3802	503	−35	1	150190903726	H
		161929	−210246	115917	−35169	6340	−679	40	−1	647740012597	F
		162509	−210727	116065	−35189	6341	−679	40	−1	180951938541	F
		175849	−227590	124859	−37610	6712	−709	41	−1	181357383206	F
		178349	−230215	125959	−37840	6736	−710	41	−1	250553380833	H
		178749	−230575	126080	−37858	6737	−710	41	−1	24410609035	H
		178829	−230631	126093	−37859	6737	−710	41	−1	1120832886082	F
		178929	−230696	126107	−37860	6737	−710	41	−1	237758854284	F/H
		181729	−233616	127314	−38107	6762	−711	41	−1	67589524904	F
		182113	−233968	127434	−38125	6763	−711	41	−1	536001031332	F
	887981	−1325671	858535	−314874	71493	−10285	915	−46	1	559466805723	F
	947069	−1395579	892683	−323685	72759	−10381	918	−46	1	61387569107	H
	969581	−1441511	928579	−338252	76143	−10836	951	−47	1	590270180319	F
	998001	−1476680	946611	−343154	76888	−10896	953	−47	1	47123179965	H
	1000901	−1479665	947832	−343402	76913	−10897	953	−47	1	247691830252	H
	1005221	−1484369	949870	−343841	76960	−10899	953	−47	1	67676294257	H
	1016101	−1498545	957510	−346019	77306	−10928	954	−47	1	109150621204	H
	1016821	−1499209	957739	−346054	77308	−10928	954	−47	1	88079936959	H
	1019141	−1501713	958812	−346282	77332	−10929	954	−47	1	1935652679	H
	1021721	−1504394	959925	−346513	77356	−10930	954	−47	1	90770738098	H
	1094099	−1587040	998899	−356226	78705	−11029	957	−47	1	359104043158	F
5637721	−9384314	6883649	−2918974	788123	−140424	16500	−1232	53	−1	96400267739	H

Chapter 9

The Maximal Obstruction and $t_M(I)$

After having considered subintervals of $(1,\infty)$ where S_I is dense, and having described techniques for finding isolated points in the spectrum, we will now focus on the infimum of the spectrum $\mathscr{S}_I$. This is the reciprocal of the so-called maximal obstruction $m(I)$ of the interval and is further related to another restriction on the transfinite diameter, the monic integer Chebyshev constant, or monic integer transfinite diameter $t_M(I)$.

9.1 Definition and Basic Properties of $t_M(I)$

In the previous chapter, we defined the integer transfinite diameter $t_{\mathbb{Z}}(I)$ of an interval $I \subset \mathbb{R}$. Determining the value of $t_{\mathbb{Z}}(I)$ turned out to be a very difficult problem, with no exact value known for any interval of nonzero length less than 4.

We will now impose a further restriction on the polynomials involved: let $\mathbb{Z}_n^*[x]$ be the set of monic polynomials of degree n and $E \subset \mathbb{C}$ be compact. We define *the monic integer transfinite diameter*, or *monic integer Chebyshev constant*, of E to be the quantity

$$t_M(E) = \lim_{n\to\infty} \inf_{p_n \in \mathbb{Z}_n^*[x]} \|p_n\|_I^{\frac{1}{n}}. \tag{9.1}$$

$t_M(E)$ inherits a few properties from the other transfinite diameters.

Lemma 9.1.1. *Let $E \subset \mathbb{C}$, $I \subset \mathbb{R}$ be compact. Then*

(*a*) $E \subseteq F \implies t_M(E) \leq t_M(F)$;

(*b*) $t_M(I) \geq t_{\mathbb{Z}}(I)$;

(*c*) $|I| \geq 4 : t_M(I) = t_{\mathbb{Z}}(I) = t(I) = \frac{|I|}{4}$.

Proof. Part (a) follows straight from the definition of $t_M(E)$, while (b) reflects the fact that $t_M(I)$ is a further restriction on the polynomials. For a proof of (c), see Theorem 1.1 in [10]. □

While the monic integer transfinite diameter shares many of its properties with the other transfinite diameters, it has a few peculiar properties. They are mostly consequences of the following lemma:

Lemma 9.1.2. *Let $q(x) = a_d x^d + \ldots + a_0 \in \mathbb{Z}_n[x]$ have all its roots $\alpha_1, \ldots, \alpha_d$ in $E \subset \mathbb{C}$ and $a_d > 1$. Then*

$$a_d^{-\frac{1}{d}} \leq t_M(E).$$

Proof. Let $P_n(x) \in \mathbb{Z}_n^*[x]$. Then

$$\begin{aligned} 1 \leq \left|\mathrm{Res}_x(P_n, q)\right| &= a_d^n \prod_{i=1}^{d} |P_n(\alpha_i)| \\ &\leq a_d^n \left\|P_n\right\|_E^d. \end{aligned}$$

Rearranging gives $a_d^{-\frac{1}{d}} \leq \|P_n\|_E^{\frac{1}{n}}$. The result now follows by taking the $\liminf_{n\to\infty}$ on the righthand side. □

This lemma has some important consequences. Firstly, it shows that it is significantly easier to find lower bounds for the monic integer transfinite diameter than it was finding them in the nonmonic case. There is no need to deal with sequences of polynomials with all roots in the interval here – any single such polynomial yields a lower bound.

It also shows that we cannot get any upper bounds on $t_M(I)$ in terms of the other transfinite diameters. Recall that, for $t_{\mathbb{Z}}(I)$, we had

$$\frac{|I|}{4} \leq t_{\mathbb{Z}}(I) \leq \sqrt{\frac{|I|}{4}},$$

due to Hilbert in [29].

One consequence of this is that the integer transfinite diameter of any single point is necessarily zero. On the other hand, if we consider the rational $\frac{p}{q}$ and note that the polynomial $qx-p$ has all roots in the set $I=\left\{\frac{p}{q}\right\}$, we see that $t_M(I)\geq\frac{1}{q}>0$. Maybe even more drastic is the following example, taken from [10]: Let $E_n=\{z\in\mathbb{C}:z^n=2\}$. Then $t_M(E_n)=2^{-\frac{1}{n}}\to 1$ as $n\to\infty$, whereas $t(E_n)=t_{\mathbb{Z}}(E_n)=0$ for all $n\in\mathbb{N}$.

The strange behaviour of $t_M(E)$ does not end here, however: Consider $E_1=\left\{\frac{1}{\sqrt{2}}\right\}$, $E_2=\left\{-\frac{1}{\sqrt{2}}\right\}$. As can be shown (see [10]), $t_M(E_1)=t_M(E_2)=0$. Taking $E=E_1\cup E_2$, we now have a complete set of conjugate algebraic numbers with minimal polynomial x^2-2 in the set, so that $t_M(E)\geq\frac{1}{\sqrt{2}}$. This behaviour generalises to arbitrary incomplete sets of conjugate algebraic numbers:

Theorem 9.1.1. *Let $S\subset\mathbb{C}$ be a finite set of irrational numbers not containing a complete set of conjugate algebraic numbers. Then $t_M(S)=0$.*

A proof of this result can be found in [10].

9.2 The Maximal Obstruction

From Lemma 9.1.2, it is clear that calculating lower bounds for the monic integer transfinite diameter is much easier than for its non-monic counterpart. Seeing that any non-monic polynomial in $\mathbb{Z}[x]$ with all roots in the compact set E gives rise to a lower bound for $t_M(E)$, we define the following:

Definition 9.2.1 (Maximal Obstruction)**.** Let $E\subset\mathbb{C}$ be compact. Then the **maximal obstruction** of E is the quantity

$$m(E)=\sup_{q(x)}a_d^{-\frac{1}{d}},$$

where the supremum is taken over all polynomials $q(x)=a_dx^d+\ldots+a_0\in\mathbb{Z}_d(E)$ with $a_d>1$.

From Lemma 9.1.2, it is clear that $m(E)\leq t_M(E)$.

In some cases, this maximal obstruction is easily calculated: if we find a polynomial $P\in\mathbb{Z}_n^*[x]$ with $\|P\|_E^{\frac{1}{\partial P}}=m(E)$, then we say that the maximal obstruction is *attained*

and we have

$$m(E) \leq t_M(E) \leq \|P\|_E^{\frac{1}{\partial P}} = m(E)$$

so that we have not only determined $m(E)$, but also found the exact value of $t_M(E)$. This works for a number of "standard" intervals, as the following list shows:

- $E = [0,1]$: Here, $\frac{1}{2} \leq t_M(E) \leq \|x(1-x)\|_E^{\frac{1}{2}} = \frac{1}{2}$.
- $E = \left[0, \frac{1}{n}\right], n > 1$: We have $\frac{1}{n} \leq t_M(E) \leq \|x\|_E = \frac{1}{n}$
- A similar argument also shows that $t_M\left(\left[-\frac{1}{n}, \frac{1}{n}\right]\right) = \frac{1}{n}$.

Using these results, together with Proposition 8.3.1, we can extend these results to a few additional intervals, getting – among others – the following results:

- $E = [n, n+1] : t_M(E) = m(E) = \frac{1}{2}$.
- $E = [n, n+2] : t_M(E) = m(E) = t_M([-1,1]) = \sqrt{t_M([0,1])} = \frac{1}{\sqrt{2}}$ (using the map $x \mapsto x^2$).
- $E = \left[-\frac{1}{\sqrt{n}}, \frac{1}{\sqrt{n}}\right] : t_M(E) = m(E) = \sqrt{t_M\left(\left[0, \frac{1}{n}\right]\right)} = \frac{1}{\sqrt{n}}$.

While these relations appeared in [10] already, a full list of relations up to degree 100 between intervals of length less than 4 can be found in Table B.1.

There are, however, sets E where a polynomial attaining the maximal obstruction is not easily calculated, and this method cannot be used. To determine the maximal obstruction for such E, we simply use the techniques of section 8.4, finding a (nonmonic) polynomial with small supremum norm on the interval. We then know that any critical polynomial $q(x) = a_d x^d + \ldots + a_0$ with $a_d^{-\frac{1}{d}} > \|P\|_E^{\frac{1}{\partial P}}$ has to appear as a factor of P, giving the polynomial for the maximal obstruction. On the interval $[0,1]$, it is enough to note that

$$P(x) = x(1-x)(1-2x)$$

satisfies $\|P\|_{[0,1]}^{\frac{1}{3}} < \frac{1}{2}$ to show that $m([0,1]) = \frac{1}{2}$.

Consider now an interval $I \subset \mathbb{R}$ not containing an integer in its interior. Then there exists a unique minimal integer $q > 1$ such that $\frac{p}{q} \in I$ for some $p \in \mathbb{Z}$. Then $I \subseteq \left[\frac{a_1}{a_2}, \frac{b_1}{b_2}\right]$ with $a_2 b_1 - b_2 a_1 = 1$, the smallest Farey interval of order $q-1$ containing I. In [27], Hare and Smyth show that, unless I contains one of the endpoints of this Farey interval, $m(I) = \frac{1}{q}$. In particular, they show the following:

Proposition 9.2.1 (Hare & Smyth)**.** *Let $I \subset \mathbb{R}$ be an interval not containing an integer in its interior, and let $\left[\frac{a_1}{a_2}, \frac{b_1}{b_2}\right]$ be the minimal Farey Interval containing I. Then*

$$m(I) = \begin{cases} \frac{1}{a_2} & \text{if } \frac{a_1}{a_2} \in I, \frac{b_1}{b_2} \notin I, a_2 > 1 \\ \frac{1}{b_2} & \text{if } \frac{a_1}{a_2} \notin I, \frac{b_1}{b_2} \in I, b_2 > 1 \\ \frac{1}{\min\{a_2, b_2\}} & \text{if } a_2, b_2 > 1, I = \left[\frac{a_1}{a_2}, \frac{b_1}{b_2}\right] \\ \frac{1}{a_2 + b_2} & \text{else} \end{cases}$$

The statement of this proposition is almost longer than its proof: one simply looks at the polynomial

$$P(x) = (b_2 x - b_1)^{m_1} (a_2 x - a_1)^{m_1} ((a_2 + b_2)x - (a_1 + b_1))^{m_2}$$

and shows that there is a choice of $m_1, m_2 \in \mathbb{N}$, so that $\|P\|_I^{\frac{1}{2m_1+m_2}} < \frac{1}{a_2+b_2}$, from which the result follows. For details of the argument, see [27].

Unfortunately, no such general results are known for intervals containing integers in their interior, or for larger intervals. It is not even known whether every interval of length less than 4 has a maximal obstruction. A few results can be obtained by relating larger intervals to ones covered by the theorem using the relations in Table B.1. While the results in the table are stated for transfinite diameters, they also apply to maximal obstructions: if $P(x) \in \mathbb{Z}_n^*[x]$ equioscillates on I_1, $P(I_1) = I_2$, and I_1 has maximal obstruction $q(x)$, then $q \circ P$ is a maximal obstruction polynomial for I_2.

The interval $I = \left[0, \frac{4}{3}\right]$, for example, has maximal obstruction $7^{-\frac{1}{3}}$, as can be seen from the identity $m([-s, s])^2 = m([0, s^2])$, applied to the following intervals:

$$m\left(\left[0, \tfrac{4}{3}\right]\right) = m\left(\left[-\tfrac{2}{3}\sqrt{3}, \tfrac{2}{3}\sqrt{3}\right]\right)^2,$$
$$m\left(\left[0, \tfrac{4}{27}\right]\right) = m\left(\left[-\tfrac{2}{9}\sqrt{3}, \tfrac{2}{9}\sqrt{3}\right]\right)^2.$$

As the two intervals on the right are connected through a cubic polynomial and $m\left(\left[0,\frac{4}{27}\right]\right)=\frac{1}{7}$ by Lemma 9.2.1 above, we see that $\left[0,\frac{4}{3}\right]$ has maximal obstruction $7^{-\frac{1}{3}}$, with polynomial $q(x)=7x^3-14x^2+7x-1$. Further, Table 9.1 shows that $t_M\left(\left[0,\frac{4}{27}\right]\right)=\frac{1}{7}$ as well, so that the maximal obstruction $m\left(\left[0,\frac{4}{3}\right]\right)$ is attained on the interval.

While it appears that, once one has found the maximal obstruction $m(E)$ for E, calculating $t_M(E)$ is simply a matter of finding the right polynomial P with $\|P\|_E^{\frac{1}{\partial P}}=m(E)$, this is not always the case. In the same paper, Hare and Smyth showed that the interval $I=[-0.684,0.517]$ has maximal obstruction $7^{-\frac{1}{3}}$, arising from the polynomial $q(x)=7x^3+4x^2-2x+1$, but that there is no $P(x)\in\mathbb{Z}^*[x]$ with $\|P\|_I^{\frac{1}{\partial P}}=7^{-\frac{1}{3}}$. This is not a unique situation either, as the following (simplified) proposition from [27] shows:

Proposition 9.2.2 (Hare & Smyth)**.** *Let $I\subset\mathbb{R}$ and $q(x)=a_dx^d+\ldots+a_x\in\mathbb{Z}_d(I), a_d>1$. If a_d is square-free, and there exists some $P\in\mathbb{Z}^*[x]$ with $\|P\|_I^{\frac{1}{\partial P}}=a_d^{-\frac{1}{d}}$, then $\frac{1}{a_d}(q(x)-q(0))\in\mathbb{Z}[x]$.*

In the situation above, the problem is that, $\frac{1}{7}(7x^2-4x^2+2x)$ does not have integer coefficients, keeping the maximal obstruction from being attained on this interval.

This of course does not mean that, for intervals of this type, $m(I)<t_M(I)$. It is conceivable that, as in the nonmonic case, $t_M(I)$ is not attained by an actual polynomial, but by an infinite product of polynomials.

As we will see later, the maximal obstruction of an interval does indeed not tell the whole story for all intervals: in Section 9.3.3, we will construct a sequence of intervals with maximal obstructions tending to 0, but $t_M(I)$ arbitrarily close to $\frac{1}{2}$. To show this, we need to analyse the behaviour of $t_M([0,x])$ when viewed as a function of $x>0$.

9.3 $t_M([0,b]), b<1$

In [27], the authors consider intervals of the form $I=[0,b]$, $\frac{1}{n}<b<\frac{1}{n-1}$ for some $n>2\in\mathbb{N}$. By lemma 9.2.1, $m(I)=\frac{1}{n}$. Based on the examples above, the authors are led to conjecture that for these intervals, $t_M(I)=m(I)$. In this section, we will show that $t_M([0,b])$, when seen as a function of $b\in\mathbb{R}_{>0}$ is continuous and use this to

disprove the conjecture.

For reference, we define the real-valued function

$$t_M(x) = t_M([0,x]), \quad x > 0.$$

We know the values of $t_M(x)$ at $x = \frac{1}{n}, n \in \mathbb{N}$, but determining $t_M(x)$ for values between reciprocals of integers is much harder. Thus, we will instead look at the analytic properties of this function. Note that the following can also be found in [30] and will be included here for completeness.

9.3.1 Continuity of $t_M(x)$

To study the behaviour of $t_M(x)$, it is useful to look back at the classical paper [9] of Borwein and Erdélyi in the theory of the (non-monic) transfinite diameter. In this paper, the authors define the function $t_{\mathbb{Z}}(x)$ in the equivalent way and state that this function is continuous, though without the details of the proof.

Let $T_n(x)$ be the n^{th} Chebyshev polynomial on $[-1,1]$, defined in 6.1. By using De Moivre's Theorem, rewritten as

$$\cos n\theta = \tfrac{1}{2}\left[(\cos\theta + i\sin\theta)^n + (\cos\theta - i\sin\theta)^n\right].$$

$T_n(x)$ can then be written as

$$T_n(x) = \tfrac{1}{2}\left[\left(x+\sqrt{x^2-1}\right)^n + \left(x-\sqrt{x^2-1}\right)^n\right].$$

From this it immediately follows that

$$T_n(x) \leq \left(x+\sqrt{x^2-1}\right)^n \text{ for } x \geq 1. \tag{9.2}$$

We will also need Chebyshev's inequality from [8]:

Lemma 9.3.1. *Let $q \in \mathbb{R}_n[x]$. Then, for $x \in \mathbb{R}\setminus[-1,1]$,*

$$\left|q(x)\right| \leq \left|T_n(x)\right| \|q\|_{[-1,1]}. \tag{9.3}$$

Proof. Without loss of generality, assume $\|q\|_{[-1,1]} = 1$ and suppose that there exists some $x_0 \in \mathbb{R}\backslash[-1,1]$ such that $|q(x_0)| > |T_n(x_0)|$. Then, for $\lambda = \frac{T_n(x_0)}{q(x_0)}$, consider the polynomial $s(x) = T_n(x) - \lambda q(x) \in \mathbb{R}_n[x]$. We have

$$\begin{aligned} |T_n(x) - s(x)| &= \left|\lambda q(x)\right| \\ &\leq \lambda \|q\|_{[-1,1]} < 1, \end{aligned}$$

so that if follows from the equioscillation that $s(x)$ has n zeros in $[-1,1]$. Seeing that also $s(x_0) = 0$, but that $\partial s(x) = n$, we are forced to conclude that $s(x) \equiv 0$. □

We can then prove:

Lemma 9.3.2. *Let $b > 0$, $p_n \in \mathbb{R}_n[y]$. Then, for every $\delta > 0$, there exists $k_{b,\delta}$, not depending on n, such that*

$$\|p_n\|_{[0,b+\delta]} \leq (1 + k_{b,\delta})^n \|p_n\|_{[0,b]}, \tag{9.4}$$

with $\lim_{\delta \to 0} k_{b,\delta} = 0$ for fixed b.

Proof. Given $p_n \in \mathbb{R}_n[y]$, let $y \in [0,b]$ and $x = \frac{2}{b}y - 1$. Then $x \in [-1,1]$. Put $q_n(x) = p_n(y)$. Then, by Lemma 9.3.1, for $x \notin [-1,1]$, $y \notin [0,b]$, we have

$$\begin{aligned} |p_n(y)| = |q_n(x)| &\leq |T_n(x)| \, \|q_n\|_{[-1,1]} \\ &= \left|T_n\left(\tfrac{2}{b}y - 1\right)\right| \|p_n\|_{[0,b]}. \end{aligned}$$

Note also that

$$\begin{aligned} \max_{y \in [b,b+\delta]} \left|T_n\left(\tfrac{2}{b}y - 1\right)\right| &= \max_{x \in [1,1+2\frac{\delta}{b}]} |T_n(x)| \\ &= \|T_n\|_{[1,1+2\frac{\delta}{b}]}. \end{aligned}$$

This clearly implies that

$$\|p_n\|_{[b,b+\delta]} \leq \|T_n\|_{[1,1+2\frac{\delta}{b}]} \|p_n\|_{[0,b]}.$$

Using inequality (9.2) above, we see that

$$\|T_n\|_{[1,1+2\frac{\delta}{b}]} \leq \left(1+2\frac{\delta}{b}\left(1+\sqrt{1+\frac{b}{\delta}}\right)\right)^n.$$

The result now follows by letting $k_{b,\delta} = 2\frac{\delta}{b}\left(1+\sqrt{1+\frac{b}{\delta}}\right) > 0$ and observing that

$$\begin{aligned}\|p_n\|_{[0,b+\delta]} &= \max\left\{\|p_n\|_{[0,b]}, \|p_n\|_{[b,b+\delta]}\right\} \\ &\leq \max\left\{\|p_n\|_{[0,b]}, (1+k_{b,\delta})^n \|p_n\|_{[0,b]}\right\} \\ &= (1+k_{b,\delta})^n \|p_n\|_{[0,b]}.\end{aligned}$$

□

Using this inequality, we also get that, for $b,\delta>0$ fixed,

$$\|p_n\|_{[0,b-\delta]} \geq \|p_n\|_{[0,b]} \left(\frac{1}{1+k_{b-\delta,\delta}}\right)^n. \tag{9.5}$$

Note also that $\lim_{\delta\to 0} k_{b-\delta,\delta} = 0$.

For $t_{\mathbb{Z}}$, Pritsker further noted that similar results can be obtained for compact subsets of the complex plane (see Lemma 5.3 in [38]).

We can now use Lemma 9.3.2 to prove continuity of $t_M(x)$.

Theorem 9.3.1. *The function $t_M(x)$ is continuous on $(0,\infty)$.*

Proof. First, note that $t_M(x)$ is (non-strictly) increasing in x. Let $b\in(0,\infty)$, $\epsilon>0$ and choose $\delta = \min\{\delta_1,\delta_2\}$, where δ_1 is chosen such that $k_{b,\delta_1} < \frac{\epsilon}{t_M(b)}$ and δ_2 is such that $\frac{k_{b-\delta_2,\delta_2}}{1+k_{b-\delta_2,\delta_2}} < \frac{\epsilon}{t_M(b)}$.

Let $0<|b-x|<\delta$. The argument splits into two cases:

(1) Suppose that $0<b-x<\delta\leq\delta_1$. Since $t_M(x)$ is increasing, we have

$$\begin{aligned}0 \leq t_M(x) - t_M(b) &\leq t_M(b+\delta_1) - t_M(b) \\ &= \lim_{n\to\infty}\left(\inf_{p_n\in\mathbb{Z}_n^*[x]} \|p_n\|^{1/n}_{[0,b+\delta_1]} - \inf_{p_n\in\mathbb{Z}_n^*[x]} \|p_n\|^{1/n}_{[0,b]}\right) \\ &\leq \lim_{n\to\infty}\left(\inf_{p_n\in\mathbb{Z}_n^*[x]} k_{b,\delta_1}\|p_n\|^{1/n}_{[0,b]}\right) \\ &= t_M(b)k_{b,\delta_1} < \epsilon.\end{aligned}$$

(2) Now assume that $0 < x - b < \delta \le \delta_2$. Here, we get

$$\begin{aligned} 0 \le t_M(b) - t_M(x) &\le t_M(b) - t_M(b-\delta_2) \\ &= \lim_{n\to\infty} \left(\inf_{p_n \in \mathbb{Z}_n^*[x]} \|p_n\|_{[0,b]}^{1/n} - \inf_{p_n \in \mathbb{Z}_n^*[x]} \|p_n\|_{[0,b-\delta_2]}^{1/n} \right) \\ &\le \lim_{n\to\infty} \left(\inf_{p_n \in \mathbb{Z}_n^*[x]} \left(\frac{k_{b-\delta_2,\delta_2}}{1+k_{b-\delta_2,\delta_2}} \right) \|p_n\|_{[0,b]}^{1/n} \right) \\ &= t_M(b) \frac{k_{b-\delta_2,\delta_2}}{1+k_{b-\delta_2,\delta_2}} < \epsilon \,. \end{aligned}$$

Thus, for $0 < |b-x| < \delta$, we have $|t_M(b) - t_M(x)| < \epsilon$ for any $b \in (0,\infty)$, proving continuity for $x > 0$. □

As mentioned before, Borwein and Erdélyi stated this result for the (non-monic) integer transfinite diameter. In fact, for any subset $\mathscr{A}_n[x] \subseteq \mathbb{R}_n[x]$ we let

$$t_{\mathscr{A}}(I) = \lim_{n\to\infty} \inf_{0 \not\equiv p_n \in \mathscr{A}_n[x]} \|p_n\|_I^{\frac{1}{n}} \,. \tag{9.6}$$

One can define $t_{\mathscr{A}}(x)$ in the equivalent way and the prove continuity of this function for $x > 0$ as in Theorem 9.3.1.

Using (9.4), one can obtain a new lower bound for $t_M([0,b])$, $b < 1$:

Lemma 9.3.3. *Let $I_b = [0,b]$, $b < 1$ and let $n = \max\{m \in \mathbb{N} \mid \frac{1}{m} > b\}$. Then*

$$t_M(I_b) \ge \max\left\{ \frac{1}{n+1}, \frac{b}{2(1+\sqrt{1-nb}) - nb} \right\}.$$

Proof. Let $\delta = \frac{1}{n} - b$. As can easily be seen from (9.4),

$$\begin{aligned} t_M\left([0, \tfrac{1}{n} - \delta]\right) &\ge t_M\left([0, \tfrac{1}{n}]\right) \frac{1}{1+k_{\frac{1}{n}-\delta,\delta}} \\ &= \frac{1-n\delta}{n(1+n\delta+2\sqrt{n\delta})} \\ &= \frac{b}{2-nb+2\sqrt{1-nb}} \,. \end{aligned}$$

Seeing that $\frac{1}{n+1}$ is also a lower bound, and is a larger for $b \le \frac{4(3n+1)}{(2n+1)^2}$, we get the result. □

9.3.2 Determining $b_{max}(n)$

While the maximal obstruction does not tell the whole story for intervals of the form $I=[0,b]$, $\frac{1}{n}<b<\frac{1}{n-1}$, it turns out that $t_M(x)$ is indeed constant on a large interval to the right of $\frac{1}{n}$ for these intervals. For $n\in\mathbb{N}$, define,

$$b_{\max}(n)=\sup_{b>\frac{1}{n}}\left\{b\,\middle|\,t_M(b)=\tfrac{1}{n}\right\}. \tag{9.7}$$

For $n=1$, this quantity is not finite, as $t_M(I)=1$ for $|I|\geq 4$ (see Lemma 9.1.1(c)). For $n=2$, we can use the results in [27] to obtain $1.26\leq b_{\max}(2)<1.328$. For $n>2$, we have the following:

Theorem 9.3.2. *Let $n>2\in\mathbb{N}$. Then*

$$\frac{1}{n}+\frac{1}{n^2(n-1)}<b_{\max}(n)\leq\frac{4n}{(2n-1)^2}.$$

Proof. The first inequality follows from the polynomial

$$P_n(x)=x^{n^2-2}(x^2-nx+1).$$

This polynomial, first used in [27], was shown to have the following properties:

1. $P_n\left(\frac{1}{n}\right)=\left(\frac{1}{n}\right)^{n^2}$.

2. $P_n'\left(\frac{1}{n}\right)=0$ and the polynomial has no other extrema in $\left[0,\frac{1}{n-1}\right]$.

3. $P_n(x)$ has a root $\beta_n=\frac{2}{n+\sqrt{n^2-4}}>\frac{1}{n}$, and $|P_n(x)|$ is strictly increasing in $\left(\beta_n,\frac{1}{n-1}\right)$.

These properties were used in [27] to show that $\|P_n\|_{[0,\frac{1}{n}+\epsilon]}=\left(\frac{1}{n}\right)^{n^2}$ for some $\epsilon>0$.

Evaluating $P_n(x)$ at $x=\frac{1}{n}+\frac{1}{n^2(n-1)}$ gives

$$\left|P_n\left(\frac{1}{n}+\frac{1}{n^2(n-1)}\right)\right|=\left(\frac{n^2-n+1}{n^2(n-1)}\right)^{n^2}\frac{n^3-3n^2+2n-1}{(n^2-n+1)^2}.$$

To show that this is indeed less than $(\frac{1}{n})^{n^2}$, first note that the sequence

$$\left\{\left(\frac{n^2-n}{n^2-n+1}\right)^{n^2}\right\}_{n=1}^{\infty}$$

is increasing, as can easily be seen by noting that $f(n) = \frac{n^2-n}{n^2-n+1}$ is an increasing function (consider the derivative of $f(x)$ for $x > 1$).

Consequently, we have

$$\left(\frac{n^2-n}{n^2-n+1}\right)^{n^2} \geq \left(\frac{2}{3}\right)^4 \text{ for } n > 2. \tag{9.8}$$

Further, note that for all n,

$$\left(\frac{2}{3}\right)^4 > \frac{n^3-3n^2+2n-1}{(n^2-n+1)^2}. \tag{9.9}$$

Thus taking (9.8) and (9.9) together, we have, for $n > 2$,

$$\left(\frac{n^2(n-1)}{n(n^2-n+1)}\right)^{n^2} > \frac{n^3-3n^2+2n-1}{(n^2-n+1)^2}.$$

Rearranging now gives the desired result.

For the upper bound, one has to look directly at (9.4). Suppose we have some $p_d(x) \in \mathbb{Z}_d^*[x]$ such that $\|p_d\|_{I_{\delta_n}}^{\frac{1}{d}} = \frac{1}{n}$ on an interval $I_{\delta_n} = [0, \frac{1}{n-1} - \delta_n]$.

Clearly, $\|p_d\|_{[0,\frac{1}{n-1}]}^{\frac{1}{d}} \geq \frac{1}{n-1}$ since $\frac{1}{n-1} \leq t_M\left([0, \frac{1}{n-1}]\right)$. Thus, using (9.4), we get

$$\frac{1}{n-1} \leq \frac{1}{n}\left(1 + k_{\frac{1}{n-1}-\delta_n,\delta_n}\right). \tag{9.10}$$

Recall that $k_{b,\delta} = \frac{2}{\delta}\left(1 + \sqrt{1+\frac{\delta}{b}}\right)$ (see the proof of from Lemma 9.3.2). Using this with $b = \frac{1}{n-1} - \delta$, we get

$$k_{\frac{1}{n-1}-\delta,\delta} = \frac{2\left(\delta(n-1) + \sqrt{\delta(n-1)}\right)}{\delta(n-1)-1}. \tag{9.11}$$

From this and (9.10), we see that

$$\frac{1}{n-1} = \frac{1}{n}\left(1 + k_{\frac{1}{n-1}-\delta_{\min},\delta_{\min}}\right),$$

where

$$\delta_{\min} = \frac{1}{(n+1)(2n+1)^2}.$$

Thus, we get

$$b_{\max}(n) \le \frac{1}{n-1} - \delta_{\min}(n) = \frac{4n}{(2n-1)^2}. \qquad \square$$

Using computational methods following the methods in Section 8.4, we get improved lower bounds for $b_{\max}(n)$ for $n = 3,\dots,9$. This is done by finding a polynomial $P_n(x) \in \mathbb{Z}_n^*[x]$ with $\|P_n\|_{[0,b)} = \frac{1}{n}$, so that then $b_{\max}(n) \ge b$, for $b \in \left(\frac{1}{n}, \frac{1}{n-1}\right)$ as large as possible. The polynomials P_n are given in Table 9.1. The polynomial P_3 is a corrected version of one appearing in [27], which does not have the property claimed (see also the corrigendum [28]), while P_4 appears in [27].

$$\begin{array}{lll} 0.465 \le b_{\max}(3), & 0.303 \le b_{\max}(4), & 0.241 \le b_{\max}(5), \\ 0.184 \le b_{\max}(6), & \frac{4}{27} \le b_{\max}(7), & 0.130 \le b_{\max}(8), \\ & 0.119 \le b_{\max}(9). & \end{array}$$

As n gets larger, computations become increasingly difficult, as the difference $\frac{1}{n-1} - \frac{1}{n}$ becomes too small.

In order to improve the lower bounds for $b_{\max}(n)$ given in Theorem 9.3.2, we need to turn to computational methods to attempt to find a monic polynomial $P(x) = \prod_{i=1}^{n} p_i(x)^{a_i} \in \mathbb{Z}^*[x]$ attaining the maximal obstruction on an interval $[0,b)$ with $\frac{1}{n} < b < \frac{1}{n-1}$. These come in two stages:

1. Using a modification of the LLL algorithm to find factors $p_i(x)$ of $P(x)$.

2. Using the linear programming methods from section 8.3.2 with additional equality constraints from [27] to determine the exponents a_i.

We will briefly discuss the implementations of both parts of the algorithm.

1. Here, we use the LLL algorithm introduced in section 8.3.2 with a modified inner product. In [10], the authors used the Lattice $\mathbb{Z}_n[x]$ with the basis $\boldsymbol{b} = (1, x, x^2, \ldots, x^n)$ and the inner product

$$\langle f_n, g_n \rangle = \int_a^b f_n(x) g_n(x) dx + a_n b_n$$

for $f_n(x) = a_n x^n + \cdots + a_0, g_n(x) = b_n x^n + \cdots + b_0 \in \mathbb{Z}_n[x]$. The additional factor $a_n b_n$ is used to discourage non-monic elements from appearing, and the algorithm usually produces only one monic basis element of degree n.

In detail, we used the following recursive algorithm to identify factors $p_i(x)$ of $P(x)$ for an interval $I = [a, b]$ where the maximal obstruction polynomial $q(x) = a_d x^d + \cdots + a_0$ is known:

   (a) Start with $\boldsymbol{b} = (1, x, x^2, \cdots, x^{20})$ (in some cases, a larger basis was required initially).

   (b) Run LLL, generating a list of factors $l = \{p_i(x)\}$.

   (c) Sieve the list by using the condition that if $p_i(x) \mid P(x)$, the resultant has to satisfy $|\mathrm{Res}_x(p_i, q)| = 1$ (see [27]).

   (d) For every p_i still in l, define

$$\widehat{\boldsymbol{b}}_i = (1, p_i(x), p_i(x)x, p_i(x)x^2, \cdots p_i(x)x^k)$$

   and re-run the LLL Algorithm with this basis, adding new factors to l.

   (e) Repeat steps (a)–(d) until no more new factors are found, at which point we return l.

2. To determine the exponents $\alpha_i = \frac{\partial p_i}{\partial P} a_i$ of $p_i(x), 1 \le i \le N$, we use the algorithm outlined in section 8.4, with modifications from [27]. Given a list of factors

$l = \{p_i(x)\}$ from step 1, one attempts to minimise m subject to

$$\begin{aligned} &\text{(i) } \textstyle\sum_{i=1}^{N} \frac{\alpha_i}{\partial p_i} \log|p_i(x)| \leq m - g(x), \quad \text{for } x \in X, \\ &\text{(ii) } \textstyle\sum_{i=1}^{N} \alpha_i = 1, \\ &\text{(iii) } \textstyle\sum_{i=1}^{N} \frac{\alpha_i}{\partial p_i} \frac{f'(\beta_s)}{f(\beta_s)} = 0, \quad 1 \leq s \leq \partial q, \text{where } q(\beta_s) = 0, \\ &\text{(iv) } \alpha_i \geq 0, \qquad 1 \leq i \leq N, \end{aligned} \tag{9.12}$$

over a finite set $X \subset I$. Here, $g(x)$ is a function such that

$$g(x) = \begin{cases} 0 & \text{if} \quad q(x) = 0 \\ \epsilon(x) > 0 & \text{if} \quad q(x) \neq 0 \end{cases},$$

where $\epsilon(x)$ is small for all $x \in I$.

The use of this function is theoretically not necessary, but is useful when doing computations, as it avoids having to deal with exact values at points where the polynomial does not need to attain the maximal obstruction.

The first two constraints in (9.12) are the same as in the non-monic case, while the third is unique to the monic case and taken from [27]. This is also where we get the final set of constraints:

Let β_s be a root of $q(x)$ and define $\hat{f}_i^{(s)} = \frac{1}{\partial f_i} \log|f_i(\beta_s)|$. If $b_1 = -\frac{1}{d}\log|a_d|, b_2, \ldots, b_l$ is an independent generating set for the $\mathbb{Z}$-lattice generated by $-\frac{1}{d}\log|a_d|$ and the $\hat{f}_i^{(s)}$, let $c_{j,i}^{(s)}$ be such that

$$\sum_{j=1}^{l} c_{j,i}^{(s)} b_j = \hat{f}_i^{(s)}.$$

Then we get the additional conditions, derived in [27]:

$$\sum_{i=1}^{N} c_{j,i}^{(s)} \alpha_i = \begin{cases} -\frac{1}{\partial q} & \text{if} \quad j = 1 \\ 0 & \text{if} \quad j > 1 \end{cases} \qquad \text{for } 1 \leq s \leq \partial q. \tag{9.13}$$

Again, we use a recursive algorithm for determining the exponents. Given a set of points X_k, we use (9.12) and (9.13) to determine the optimal exponents $\boldsymbol{\alpha}_k = \left(\alpha_1^{(k)}, \alpha_2^{(k)}, \ldots, \alpha_N^{(k)}\right)$ attaining the minimum value m_k. We then construct the function

$$f(x, \boldsymbol{\alpha}_k) = \sum_{i=1}^{N} \frac{\alpha_i^{(k)}}{\partial f_i} \log|f_i(x)|,$$

and add its minima to X_k to obtain X_{k+1} and set $M_k = \inf_{x \in I} f(x, \boldsymbol{\alpha}_k)$. As in the non-monic case, starting with a small set of values $X_1 \subset I$, we repeat this procedure until we get $K \in \mathbb{N}$ such that $m_K - M_K < \epsilon$ for required precision $\epsilon > 0$. In this case, we used Maple's `RootFinding[Isolate]` to trap the roots of the derivative, and then used an implementation of Brent's method [37] to determine the location of the minima of $-f(x, \boldsymbol{\alpha})$ to high precision. Finally, we verify that $e^{M_K} = |a_d|^{-\frac{1}{d}}$.

One can attempt to find rational approximations of smaller denominator to the exponents (which is not always possible), always checking that the obstruction is still attained. The attaining polynomial $P(x)$ is then found by clearing denominators in the exponents of $P_K(x) = \exp(f(x, \boldsymbol{\alpha}_K))$.

The polynomials attaining the obstructions obtained this way can be found in Table 9.1.

9.3.3 Intervals where $t_M(I) - m(I)$ is large

As discussed before, the continuity of the function $t_M(x), x > 0$ has some important implications for the monic integer transfinite diameter of intervals $[0, b]$, where b is close to $\frac{1}{n}, n \in \mathbb{N}$.

One can use this idea to produce intervals where the classical lower bound (the maximal obstruction) is very far from the actual value of the monic integer transfinite diameter, as follows:

Let $n > 1 \in \mathbb{N}$, $0 \leq a < \frac{1}{n}$ and consider the interval $\left[a, \frac{1}{n} - \delta\right]$ for $\delta < \frac{1}{n} - a$. From a simple generalisation of (9.4), one can show that

Table 9.1: Extremal monic polynomials $P_n(x)$ with $\|P_n\|_{[0,b_n]}^{\frac{1}{\partial P_n}} = \frac{1}{n}$

n	$p_{n,i}(x)$	$\alpha_{n,i}$	b_n
3	$x^{14}-1140262261x^{13}+47054086x^{12}-884563310x^{11}+100247244x^{10}-76341256x^9+41208853x^8$		
	$-16202606x^7+4692047x^6-999261x^5+154318x^4-16766x^3+1211x^2-52x+1$	2450525	
	$x^8+14184x^7-34944x^6+36442x^5-20832x^4+7041x^3-1405x^2+153x-7$	877415	
	$x^8+4842x^7-10935x^6+10355x^5-5317x^4+1594x^3-278x^2+26x-1$	2571030	
	$x^8+7812x^7-18072x^6+17561x^5-9271x^4+2864x^3-516x^2+50x-2$	595980	.456
	$x^7-1233x^6+2406x^5-1913x^4+791x^3-179x^2+21x-1$	1210840	
	$x^5-3x^4+7x^3-11x^2+6x-1$	1052898	
	x	45944640	
4	$x^7+8760x^6-13342x^5+8488x^4-2784x^3+514x^2-50x+2$	47	
	$x^5+432x^4-456x^3+179x^2-31x+2$	35	.303
	x	640	
5	$x^{12}+131010440x^{11}-273704878x^{10}+258285423x^9-145270543x^8+54088464x^7$		
	$-13992205x^6+2565036x^5-333045x^4+29998x^3-1784x^2+63x-1$	3228968042433	
	$x^9+644400x^8-996660x^7+669586x^6$		
	$-255106x^5+60255x^4-9030x^3+838x^2-44x+1$	4370984625200	.241
	$x^4+120x^3-74x^2+15x-1$	345995793198	
	x	90627835142196	
6	$x^7-140190x^6+132517x^5-51966x^4+10819x^3-1261x^2+78x-2$	200917	
	$x^5+1260x^4-852x^3+215x^2-24x+1$	118824	.184
	x	5232473	
7	$x^5+3472x^4-1826x^3+358x^2-31x+1$	1	$\frac{4}{27}$
	x	44	
8	$x^4-576x^3+208x^2-25x+1$	3	
	x^2-8x+1	1	.130
	x	50	
9	$x^{10}-397139760x^9+399672846x^8-178374477x^7+46335369x^6$		
	$-7720161x^5+855561x^4-63062x^3+2981x^2-82x+1$	193221	
	$x^9-27204336x^8+26039934x^7-10845660x^6+2568351x^5$		
	$-378358x^4+35516x^3-2075x^2+69x-1$	32130	
	$x^7+1078992x^6-721970x^5+200827x^4-29722x^3+2468x^2-109x+2$	184212	.119
	x	11410308	

$$t_M\left(\left[a,\frac{1}{n}\right]\right) \leq \left(1+k_{a,\frac{1}{n}-\delta,\delta}\right) t_M\left(\left[a,\frac{1}{n}-\delta\right]\right) \tag{9.14}$$

where

$$k_{c,d,\delta} = \frac{2\delta}{d-c}\left(1+\sqrt{1+\frac{d-c}{\delta}}\right).$$

From rearranging (9.14) and using the expression of $k_{a,\frac{1}{n}-\delta,\delta}$, we get a lower bound on $t_M([a,\frac{1}{n}-\delta])$:

$$t_M\left(\left[a,\frac{1}{n}-\delta\right]\right) \geq m\left(\left[a,\frac{1}{n}\right]\right)\frac{\delta n+an-1}{an-\delta n-1-2\sqrt{\delta n(1-an)}} \tag{9.15}$$

Using this, we get the following result:

Lemma 9.3.4. *Let $n \geq 2, \epsilon > 0$ and let $\left[a,\frac{1}{n}\right]$ be a Farey interval. Then, for $0 < \delta < n(1-an)\left(\frac{\epsilon}{n\epsilon-2}\right)^2$,*

$$t_M\left(\left[a,\frac{1}{n}-\delta\right]\right) > \frac{1}{n}-\epsilon$$

Proof. This is easily verified using (9.14) with $\delta < n(1-an)\left(\frac{\epsilon}{n\epsilon-2}\right)^2$ and using the fact (Lemma 9.2.1), that $m\left(\left[\frac{p}{q},\frac{r}{s}\right]\right) = \max\left\{\frac{1}{q}.\frac{1}{s}\right\}$ if $rq-ps=1$. □

We can use this to construct intervals I where the maximal obstruction $m(I)$ is far from being the correct value of $t_M(I)$.

Consider the intervals $I_k = \left[\frac{k}{2k+1},\frac{1}{2}-\delta\right]$ for $\delta > 0, k \in \mathbb{N}$. Since the Farey interval $\left[\frac{k}{2k+1},\frac{1}{2}\right]$ contains I_k and, as can easily be checked, is the smallest Farey interval containing I_k, it follows from Lemma 9.2.1 that $m(I_k) = \frac{1}{2k+1}$. But, the above Lemma shows that, for δ sufficiently small, we can have $t_M(I_k)$ arbitrarily close to $\frac{1}{2}$.

Appendix A

Computing the Inverse Vandermonde Matrix

When defining the polynomial representation of an equivalence class of algebraic n-tuples, we came across the problem of inverting the Vandermonde matrix.

Let K be a field, $x_1, \ldots, x_n \in K$ be distinct. We are interested in finding the inverse of the matrix

$$\boldsymbol{V}(x_1, \ldots, x_n) = \begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{bmatrix}$$

explicitly.

We define the coefficient vector of a polynomial $p(z) = a_d z^d + \ldots + a_0 \in K[z]$ to be the vector $(a_0, \ldots, a_d) \in K^{d+1}$.

Lemma A.0.5. *Let $q(z) = \prod_{i=1}^{n}(z - x_i)$. The i^{th} column of the right inverse of $\boldsymbol{V}(x_1, \ldots, x_n)$ is given by the coefficient vector of the polynomial*

$$\frac{q(z)}{(z - x_i)q'(x_i)}. \tag{A.1}$$

Proof. First, note that this is indeed a polynomial in $K[z]$: we may write $q(z) =$

$(z - x_i)s(z)$, where $s(z) = \prod_{i \neq j}(z - x_j) \in K[z]$.

Further, as the derivative $q'(z) = s(z) + (z - x_i)s'(z)$, we see at once that $s(x_i) = q'(x_i)$, so that

$$\left.\frac{q(z)}{(z - x_i)q'(x_i)}\right|_{z=x_i} = \frac{s(x_i)}{q'(x_i)} = 1$$

On the other hand, for $j \neq i$, we have

$$\left.\frac{q(z)}{(z - x_i)q'(x_i)}\right|_{z=x_j} = \frac{0}{(x_j - x_i)q'(x_i)} = 0.$$

□

For alternative methods, see [13] or [40].

Appendix B

B.1 Irreducibility of the generalised Gorškov polynomials

In our discussion of the generalised Gorškov polynomials, we used the irreducibility of the polynomials $g_k^{(b)}(x)$, $b \equiv 1 \pmod 2$ without proof. We will now provide the missing proof, following the argument in [42] and filling in details as needed. Unfortunately, the argument from Theorem 7.2.1 does not carry over in this case, as no 3-term recurrence relation as in (7.16) exists for the $g_k^{(b)}(x)$. To prove irreducibility in this case, we have to resort to a more sophisticated argument. We start with a nice lemma from [5]:

Proposition B.1.1 (Albert 1956)**.** *Let p be prime, $\mathbb{F}_p$ be the finite field pf p elements, and $\gamma \in \mathbb{F}_{p^n}$ for some $n \in \mathbb{N}$. Then the equation*

$$x^p - x - \gamma = 0$$

has solutions in $\mathbb{F}_{p^n}$ if and only if $\mathrm{Tr}_{\mathbb{F}_p} \gamma \neq 0$.

To prove this, we will need two Lemmas, both from [5]. The first is a result about a certain class of polynomials over a field of prime characteristic:

Lemma B.1.1. *Let p be prime and $a \in \mathbb{F}_p$. Then the polynomial $f(x) = x^p - x - a$ is reducible if and only if $f(x) = 0$ has a solution in $\mathbb{F}_p$.*

Proof. Suppose $f(x)$ has a root ζ and consider $\zeta + k$, $k = 0, \ldots, p-1$. We have

$$\begin{aligned}(\zeta + k)^p &= \zeta^p + k^p \\ &= \zeta + k + a\end{aligned}$$

so that these are then all the roots of $f(x)$. If now $f(x) = g(x)h(x)$, with $\partial g = r < p$ and β is a root of $g(x)$, the trace of β will have the form $\mathrm{Tr}_{\mathbb{F}_p} \beta = r\zeta + s, s \in \mathbb{N}$, so that

$$\begin{aligned}\zeta &= r^{-1}(r\zeta + s) - r^{-1}s \\ &= r^{-1}\mathrm{Tr}_{\mathbb{F}_p} \beta - r^{-1}s \in \mathbb{F}_p,\end{aligned}$$

as required. The converse is trivial. □

Lemma B.1.2. *Let p be prime, $n \in \mathbb{N}$, $q = p^n$ and let $\gamma \in \mathbb{F}_q$. Then*

$$\mathrm{Tr}_{\mathbb{F}_p} \gamma = 0 \iff \gamma = \sigma_p \alpha - \alpha,$$

for some $\alpha \in \mathbb{F}_q$. Here, σ_p is the Frobenius endomorphism.

Proof. First, let us recall that the Frobenius endomorphism

$$\begin{aligned}\sigma_p : \mathbb{F}_q/\mathbb{F}_p &\to \mathbb{F}_q/\mathbb{F}_p \\ x &\mapsto x^p\end{aligned}$$

is a generator for the cyclic Galois group $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. Thus, choose a primitive root u of $x^q - x$. Then

$$u, \sigma_p u, \ldots, \sigma_p^{n-1} u$$

forms a basis for $\mathbb{F}_q/\mathbb{F}_p$. Write $\alpha = \alpha_1 u + \ldots + \alpha_n \sigma^{n-1} u$. Then $\sigma_p \alpha - \alpha$ takes the form

$$\sigma_p \alpha - \alpha = (\alpha_n - \alpha_1)u + (\alpha_1 - \alpha_2)\sigma_p u + \ldots + (\alpha_{n-1} - \alpha_n)\sigma_p^{n-1} u.$$

If we let $\gamma = \gamma_1 u + \ldots + \gamma_n \sigma_p^{n-1} u = \sigma_p \alpha - \alpha$, we see that

$$\begin{aligned}\sum_{i=1}^{n} \gamma_i &= (\alpha_n - \alpha_1) + (\alpha_1 - \alpha_2) + \ldots + (\alpha_{n-1} - \alpha_n) \\ &= 0.\end{aligned}$$

Note now that this is indeed the trace of γ, as

$$\begin{aligned}\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} \gamma &= \sum_{i=1}^{n} \sigma_p^i \gamma \\ &= (\gamma_1 + \ldots + \gamma_n)(u + \sigma_p u + \ldots + \sigma_p^{n-1} u) \\ &= \sum_{i=1}^{n} \gamma_i.\end{aligned}$$

This follows from the fact that $w = u + \ldots + \sigma_p^{n-1} u \neq 0$ satisfies the equation $x^{p^k} = x$ for every $k \in \mathbb{N}$, and therefore $w = 1$.

This shows that if $\gamma = \sigma_p \alpha - \alpha$ for some $\alpha \in \mathbb{F}_q$, it indeed has zero trace. To prove the converse, if given γ with $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} \gamma = 0$, choose α_1 arbitrary in $\mathbb{F}_p$ and solve for $\alpha_2, \ldots, \alpha_n$. □

Consider now the polynomial $f(x) = x^p - x - \gamma$, $\gamma \in \mathbb{F}_q$, $q = p^n$. Then we have

$$f(x) \text{ reducible over } \mathbb{F}_q \iff \alpha^p - \alpha = \gamma \text{ for some } \alpha \in \mathbb{F}_q \iff \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} \gamma = 0,$$

the first by Lemma B.1.1, the second from Lemma B.1.2. This completes the proof of Proposition B.1.1.

We will also need the following basic result:

Lemma B.1.3. *Let $\alpha \neq 0$ lie in a field of characteristic 2 and let $\mu = \alpha + \alpha^{-1}$ with $\mu^{2^{2^n}} = \mu$. Then $\alpha^{2^{2^n}} \in \{\alpha, \alpha^{-1}\}$.*

Proof. Using characteristic 2, we have

$$\begin{aligned}\mu^{2^{2^n}} &= \left(\alpha + \alpha^{-1}\right)^{2^{2^n}} \\ &= \alpha^{2^{2^n}} + \alpha^{-2^{2^n}},\end{aligned}$$

which equals μ by assumption. Thus, $\alpha^{2^{2^n}}$ has to be one of the two solutions of the equation $\mu = x + x^{-1}$, i.e. one of α or α^{-1}. □

We can now use these to prove the following:

Proposition B.1.2. *In $\mathbb{F}_2$, let $\gamma_0 = 1$ and, for $n \geq 1$, define*

$$\gamma_n + \gamma_n^{-1} = \gamma_{n-1}. \tag{B.1}$$

Then $[\mathbb{F}_2(\gamma_n) : \mathbb{F}_2] = 2^n$.

Proof. We will proceed by induction. First, note that for $n = 1$, the polynomial $x^2 + x + 1$ is irreducible over $\mathbb{F}_2$, so that $[\mathbb{F}_2(\gamma_1) : \mathbb{F}_2] = 2$. Further, $\gamma_1^2 = \gamma_1^{-1}$ and $\mathrm{Tr}_{\mathbb{F}_2} \gamma_1 = \gamma_1 + \gamma_1^{-1} = 1$. Suppose now that we have some $n \in \mathbb{N}$ such that the following hold:

$$\begin{aligned} [\mathbb{F}_2(\gamma_n) : \mathbb{F}_2] &= 2^n \\ \gamma_n^{2^{2^{n-1}}} &= \gamma_n^{-1} \\ \mathrm{Tr}_{\mathbb{F}_2} \gamma_n &= 1. \end{aligned} \tag{B.2}$$

Multiplying both sides of (B.1) by $\frac{\gamma_{n+1}}{\gamma_n}$ and rearranging, we get

$$\left(\frac{\gamma_{n+1}}{\gamma_n}\right)^2 + \frac{\gamma_{n+1}}{\gamma_n} + \frac{1}{\gamma_n^2} = 0. \tag{B.3}$$

Now, as we are working in a field of characteristic 2, we have $p(\gamma_n)^{2^k} = p(\gamma_n^{2^k})$ for any $k = 0, \ldots, 2^n - 1$, so that the conjugates of γ_n can be expressed as 2^k-th powers of γ_n, yielding

$$\mathrm{Tr}_{\mathbb{F}_2} \gamma_n = \sum_{i=0}^{2^n - 1} \gamma_n^{2^i}. \tag{B.4}$$

Further, the induction hypothesis gives $\gamma_n^{-2} = \gamma^{2 \cdot 2^{2^{n-1}}}$, so that $\mathrm{Tr}_{\mathbb{F}_2} \gamma_n^{-2} = \mathrm{Tr}_{\mathbb{F}_2} \gamma_n$. Applying Lemma B.1.1 to (B.3), we see that indeed

$$\begin{aligned} [\mathbb{F}_2(\gamma_{n+1}) : \mathbb{F}_2] &= [\mathbb{F}_2(\gamma_{n+1}) : \mathbb{F}_2(\gamma_n)] \cdot [\mathbb{F}_2(\gamma_n) : \mathbb{F}_2] \\ &= 2^n \cdot 2 = 2^{n+1}. \end{aligned}$$

To prove the second part of (B.2), we note that Fermat's Theorem tells us that the equation

$$x^{2^{2^n}} = x$$

has exactly 2^{2^n} solutions in $\mathbb{F}_{2^{2^n}} = \mathbb{F}_2(\gamma_n)$. Since it cannot have more solutions, $\gamma_{n+1}^{2^{2^n}} \neq \gamma_{n+1}$, which implies $\gamma_{n+1}^{2^{2^n}} = \gamma_{n+1}^{-1}$, using Lemma B.1.3.

Using characteristic 2 once again, we get $\gamma_{n+1}^{2^k} + \gamma_{n+1}^{-2^k} = \gamma_n^{2^k}$, $k = 0, \ldots, 2^n - 1$. Using $\gamma_{n+1}^{2^{2^n}} = \gamma^{-1}$ and (B.4), we see that we can write the trace of γ_{n+1} as

$$\begin{aligned}\mathrm{Tr}_{\mathbb{F}_2}\gamma_{n+1} &= \sum_{k=0}^{2^{n+1}-1} \gamma_{n+1}^{2^k} = \sum_{k=0}^{2^n-1} \gamma_{n+1}^{2^k} + \gamma_{n+1}^{-2^k} \\ &= \sum_{k=0}^{2^n-1} \gamma_n^{2^k} = \mathrm{Tr}_{\mathbb{F}_2}\gamma_n = 1,\end{aligned}$$

using the induction hypothesis. □

Finally, we can use this to prove irreducibility:

Theorem B.1.1. *Let* $\beta_0 = b \equiv 1 \pmod 2$ *and define*

$$\beta_n = \beta_{n+1} + \beta_{n+1}^{-1},\ n \geq 1.$$

Then $[\mathbb{Q}(\beta_n) : \mathbb{Q}] = 2^n$.

Proof. We will actually work over $\mathbb{Q}_2$, the 2-adic numbers and show that $[\mathbb{Q}_2(\beta_n) : \mathbb{Q}_2] = 2^n$, from which the result will follow. We will proceed by induction, using Hensel's Lemma. For $n = 0$, note that the result certainly holds.

For inductive purposes, assume that $\mathbb{Q}_2(\beta_n)$ is unramified over $\mathbb{Q}_2$ and let $f(x) = x^2 - \beta_n x + 1$. Further, let $\gamma_n \equiv \beta_n \pmod 2$, so that $\mathbb{Q}_2(\beta_n)$ has residue class field $\mathbb{F}_2(\gamma_n)$. Note that $f(\gamma_{n+1}) \equiv \gamma_{n+1}^2 - \gamma_n\gamma_{n+1} + 1 \equiv 0 \pmod 2$, while $f'(\gamma_{n+1}) \equiv \gamma_n \not\equiv 0 \pmod 2$. Hensel's Lemma thus guarantees a β_{n+1} with $f(\beta_{n+1}) = 0$ and $\beta_{n+1} \equiv \gamma_{n+1} \pmod 2$. Further, for such β_{n+1},

$$[\mathbb{Q}_2(\beta_{n+1}) : \mathbb{Q}_2(\beta_n)] \geq [\mathbb{F}_2(\gamma_{n+1}) : \mathbb{F}_2(\gamma_n)] = 2,$$

so that $\mathbb{Q}_2(\beta_{n+1})$ is unramified of degree 2^{n+1} over $\mathbb{Q}_2$. □

B.2 Relations between various subintervals of length less than 4

Given a polynomial $P(x) \in \mathbb{Z}_d[x]$ with leading coefficient b, we have

$$\tfrac{1}{b} t_{\mathscr{A}}(X) \leq \left(t_{\mathscr{A}}(P^{-1}(X))\right)^d \leq t_{\mathscr{A}}(X)$$

for any $X \subset \mathbb{C}$, as shown in [6], and is proved in proposition 8.3.1. In particular, if we take $P(x)$ to be monic, we get equality, such as in the case of $P(x) = x(1-x)$, giving the relation $t_{\mathscr{A}}([0,1]) = \sqrt{t_{\mathscr{A}}\left(\left[0, \frac{1}{4}\right]\right)}$. As this gives a way to generalise results about the various transfinite diameters (and related quantities, such as maximal obstructions), it is an interesting problem to try and determine all such relations for intervals I of length less than 4.

We immediately note that there is an important restriction on the polynomials involved: for a real interval I, in general, $P^{-1}(I) \subset \mathbb{C}$, but we want $P^{-1}(I) \subset \mathbb{R}$, we can only use polynomials equioscillating on, and with all roots in, the real interval I. Let $R(I)$ denote the set of all such relations on $I \subset \mathbb{R}$.

B.3 Relations up to degree 100

Recall that $T_n(x)$, the n^{th} Chebyshev polynomial on $[-1,1]$, is an equioscillating polynomial, and that $2^{1-n}T_n(x)$ is the monic polynomial of minimal supremum norm on $[-1,1]$. Also, by Lemma 7.1.3, $T_n(x)$ has an explicit expression

$$T_n(x) = \frac{1}{2}\left((2x)^n + \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} (-1)^k \frac{n}{k} \binom{n-k-1}{k-1} (2x)^{n-2k}\right). \tag{B.5}$$

When we proved this (along with the uniqueness of $T_n(x)$) in Theorem 6.2.2, we only used the fact that $T_n(x)$ equioscillates on the interval. Thus, any monic equioscillating polynomial $p_n(x) \in \mathbb{R}_n[x]$ on $[-1,1]$ is of the form $p_n(x) = T_n(x) + c$ for suitable $c \in \mathbb{R}$. We can use this fact to perform an exhaustive search for all monic equioscillating polynomials with integer coefficients and all roots in a subinterval

$I = [a,b] \subset [0,5]$ with $b-a<4$.

Recall that the n^{th} Chebyshev polynomial for $[a,b]$ is the monic polynomial

$$\widetilde{T_n}(x) = 2\left(\frac{b-a}{4}\right)^n T_n\left(\frac{2x-a-b}{b-a}\right).$$

Letting $\widetilde{T_n}(x) = x^n + c_{n-1}x^{n-1} + \ldots + c_0$, we can use (B.5) to deduce c_{n-1} and c_{n-2}:

$$c_{n-1} : -\frac{n}{2}(a+b)$$
$$c_{n-2} : \frac{1}{16}\left(4\binom{n}{2}(a+b)^2 - n(b-a)^2\right)$$

Now setting $c_{n-1} = -k, k>0 \in \mathbb{Z}$ and using this to eliminate a in c_{n-2} we see that a,b have to satisfy

$$a = \frac{kn - 2\sqrt{n\binom{n}{2}k^2 - un^3}}{n^2}$$
$$b = \frac{kn + 2\sqrt{n\binom{n}{2}k^2 - un^3}}{n^2},$$

where $u = c_{n-2} \geq 0$ is an integer.

Using the conditions $a>-2, b-a<4$ and the fact that the discriminant is positive, we get bounds on u in terms of n and k. By further using the fact that $k = 1,\ldots 5n-1$ (seeing that the $(n-1)^{th}$ derivative of $\widetilde{T_n}(x)$ has to have all roots in $[0,5]$), we can construct all such $\widetilde{T_n}(x)$, discarding any with nonintegral $a_{n-3},\ldots,a_1$. For the remaining polynomials, one then simply finds a suitable c so that $p_n(x) = \widetilde{T_n}(x) + c$ has integer coefficients and all roots on the real line.

We will call a relation $P(x) \in R(I)$ *primitive* if it cannot be written as a composition of other relations in $R(I)$. Using the methods described above, we can construct an exhaustive list of (non-primitive) relations between intervals of degree up to 100. The primitive relations arising from this list are shown in Table B.1.

Thus, every relation on intervals I with $|I|<4$ can be obtained through composition of the relations in the table. In particular, this includes integer shifts and reflections

around integers, but also the degree 6 relation

$$P(x) = (x+1)(x-1)(x^2-x-1)(x^2+x-1),$$

mapping $\left[-\frac{2}{3}\sqrt{6}, \frac{2}{3}\sqrt{6}\right]$ to $\left[-1, \frac{5}{27}\right]$ was omitted, as it can be written as

$$P(x) = (x^2-1)\left((x^2-1)-(x^2-1)-1\right) = P_{12}\left(P_1\left(P_3(x)\right)\right),$$

using the notation in the table.

B.4 Relations where $|I| \leq 3.7$

While the methods of the previous section cannot be used to perform an exhaustive search, we can show that the list of polynomials in Table B.1 is exhaustive in cases where $|I| \leq 3.7$. To do this, we once again recall that, if we have $P(x) \in \mathbb{Z}[x]$ with $\|P\|_I^{\frac{1}{\partial P}} < 1$, then any $q(x) \in \mathbb{Z}^*(I)$ occurs as a factor of P.

Recall too that, for every interval of length up to 4, some integer translate of the interval lies in $[-2,3]$. Thus, were there some $P(x) \in \mathbb{Z}[x]$ with $\|P\|_{[-2,3]}^{\frac{1}{\partial P}} < 1$, its factors would give an exhaustive list of all such $q(x) \in \mathbb{Z}_n^*([-2,3])$. This, of course, is not possible, as $t_{\mathbb{Z}}([-2,3]) = t([-2,3]) = \frac{5}{2}$.

We can, however, attempt to find a list of intervals I_i with $|I_i| < 4$ such that every interval of length less than some fixed l has an integer translate contained in one of the I_i. For

$$I_i = \left[-2+\tfrac{i}{10}, 1.8+\tfrac{i}{10}\right], \quad i = 0, \ldots, 12,$$

it is easy to see that every interval of length up to 3.7 can be translated by an integer to lie within one of these intervals. By using the symmetry $x \mapsto 1-x$, we can reduce this list. Table B.2 shows that each of the I_i indeed has $t_{\mathbb{Z}}(I_i) < 1$ and gives the factors of the polynomials.

Of course, this in itself does not prove that Table B.1 is exhaustive for these intervals. To prove this, we need to do the following:

1. Find a way to construct equioscillating polynomials from a list of factors

2. Use this with the polynomials in Table B.2 to construct a list of relations.

For 1., suppose that $P(x)$ is a relation on the interval I. Thus, $P(x)$ equioscillates on I and maps the interval $\partial P : 1$ to $P(I)$. In other words, for every $y \in P(I)$, $\#(P^{-1}(y)) = \partial P$. We then have:

Lemma B.4.1. *Let $P(x) \in R(I)$. Then*

$$P(x) = s(x)\,t(x)^2,$$

where $s(x), t(x) \in \mathbb{Z}^*(I)$ are square-free, and $\partial s = 0, 1,$ or 2.

Proof. First, note that if $P(x) = s(x)^n$, where $n > 2$, then for any $a \neq 0$, there is some $a \in I_2$ with $\#(P^{-1}(a)) = 1 < \partial P$. The same holds for $P(x) = s(x)\,t(x)^n$ when $n > 2$ and $s(x)$ is square-free.

Consider now the case $P(x) = s(x)\,t(x)^2$, where $s(x)$ is again square-free and $t(x)$ has d roots at $\alpha_1, \ldots, \alpha_d$. Looking at the derivative

$$P'(x) = t(x)\left(2t'(x)s(x) + s'(x)\,t(x)\right),$$

and seeing that the roots of the derivative have to interlace the roots of $P(x)$, we conclude that $\partial s(x) = 0, 1$, or 2. As is easily verified, the only possible cases are as follows:

- $s(x)$ is linear, with a root at $x = \beta$ and $\beta < \alpha_1 < \ldots < \alpha_d$, or $\alpha_1 < \ldots < \alpha_d < \beta$, or
- $s(x)$ is a quadratic with roots β_1, β_2, satisfying $\beta_1 < \alpha_1 < \ldots < \alpha_d < \beta_2$. □

Now, as any polynomial of the form $P(x) = s(x)^2$ is simply a composition of $s(x)$ with $x \mapsto x^2$ and is therefore omitted in Table B.1, we can simply restrict ourselves to looking for relations generated by polynomials with no repeated roots and polynomials of the form $P(x) = s(x)\,t(x)^2$, as described above. By constructing all relations that can be obtained this way from the factors in Table B.2, we see that Table B.1 is indeed exhaustive for all intervals $I : |I| \leq 3.7$. As it turns out, the relations never actually have any repeated roots.

All computations were done in Maple, following the algorithm in Section 8.3.2. As all factors had all their roots in the intervals in question, we simply used the roots of the factors as endpoints of intervals containing the roots of the derivative, and then used an implementation of Brent's method [37] to determine the location and value of the extrema to high precision.

Table B.1: List of primitive relations occurring as factors of relations $P(x)$ of degree up to 100 for intervals I with $|I| < 4$. $s \geq 0$ is a real parameter

n	I_1	$P_n(I)$	$P_n(x)$
1	$[a,b]$	$[a+1,b+1]$	$x-1$
2	$[a,b]$	$[-b,-a]$	$-x$
3	$[-s,s]$	$\left[0,s^2\right]$	x^2
4	$[-s,1+s]$	$\left[-s-s^2,\frac{1}{4}\right]$	$x(1-x)$
5	$[-1-s,1+s]$	$\left[-2s-s^2,1\right]$	$(1-x)(1+x)$
6	$[-1-s,2+s]$	$\left[-3s-s^2,\frac{9}{4}\right]$	$(1-x)(2-x)$
7	$\left[-\sqrt{2}-s,\sqrt{2}+s\right]$	$\left[-2,2\sqrt{2}s+s^2\right]$	x^2-2
8	$\left[-\sqrt{3}-s,\sqrt{3}+s\right]$	$\left[-3,2\sqrt{3}s+s^2\right]$	x^2-3
9	$\left[\frac{1}{2}-\frac{1}{2}\sqrt{5}-s,\frac{1}{2}+\frac{1}{2}\sqrt{5}+s\right]$	$\left[-\frac{5}{4},\sqrt{5}s+s^2\right]$	x^2-x-1
10	$\left[-\frac{2}{3}\sqrt{3},\frac{2}{3}\sqrt{3}\right]$	$\left[-\frac{2}{9}\sqrt{3},\frac{2}{9}\sqrt{3}\right]$	$x(x-1)(x+1)$
11	$\left[-\frac{2}{3}\sqrt{6},\frac{2}{3}\sqrt{6}\right]$	$\left[-\frac{4}{9}\sqrt{6},\frac{4}{9}\sqrt{6}\right]$	$x(x^2-2)$
12	$\left[-1,\frac{5}{3}\right]$	$\left[-1,\frac{5}{27}\right]$	$x(x^2-x-1)$
13	$\left[\frac{1}{3}-\frac{2}{3}\sqrt{7},\frac{1}{3}+\frac{2}{3}\sqrt{7}\right]$	$\left[-\frac{20}{27}-\frac{14}{27}\sqrt{7},-\frac{20}{27}+\frac{14}{27}\sqrt{7}\right]$	$x(x+1)(x-2)$
14	$\left[\frac{2}{3}-\frac{2}{3}\sqrt{7},\frac{2}{3}+\frac{2}{3}\sqrt{7}\right]$	$\left[-\frac{7}{27}-\frac{14}{27}\sqrt{7},-\frac{7}{27}+\frac{14}{27}\sqrt{7}\right]$	x^3-2x^2-x+1
15	$\left[\frac{1}{2}-\frac{1}{2}\sqrt{6},\frac{1}{2}+\frac{1}{2}\sqrt{6}\right]$	$\left[-\frac{1}{4},\frac{5}{16}\right]$	$(x-1)x(x^2-x-1)$
16	$\left[\frac{1}{2}-\frac{1}{2}\sqrt{10},\frac{1}{2}+\frac{1}{2}\sqrt{10}\right]$	$\left[-1,\frac{9}{16}\right]$	$(x+1)x(x-1)(x-2)$

Table B.2: Polynomials $P_j(x)$ used to prove that the list of relations in Table B.1 is exhaustive for $I : |I| \leq 3.7$. $P_j(x) = \prod_{i=1}^{28} p_i(x)^{a_{ij}}$, where a_{ij} is the i^{th} entry in the j^{th} column. The bottom row gives the (normalised) supremum norm of the polynomial.

$p_i(x)$	$[-2,1.8]$	$[-1.9,1.9]$	$[-1.8,2]$	$[-1.7,2.1]$	$[-1.6,2.2]$	$[-1.5,2.3]$	$[-1.4,2.4]$
x	321470	75340	237870	81111	65943	1654100	1647800
$x+1$	632390	59455	302080	94963	95898	1060800	1089600
$x-1$	451070	59455	616120	94081	64428	578400	589190
$x+2$	387200	0	0	0	0	0	0
$x-2$	0	0	84700	92452	81087	970530	966340
x^2-2	147760	46982	100340	63950	50695	812250	788500
x^2-3	274940	53630	315320	0	0	0	0
x^2+x-1	353980	18402	182520	69045	0	0	0
x^2-x-1	367970	18402	291200	54295	67875	464060	464060
x^3-3x+1	383570	39513	0	0	0	0	0
x^3-3x-1	0	39513	398600	58720	0	0	0
x^3+x^2-2x-1	141640	20954	149980	0	0	34033	28022
x^3-x^2-2x+1	286300	20954	109950	28887	30265	1013300	1039300
x^3-x^2-3x+1	0	0	0	0	62080	0	0
x^4-5x^2+5	0	10618	0	0	0	0	0
x^4-4x^2+2	0	31410	0	0	0	10437	0
$x^4-x^3-3x^2+x+1$	0	0	0	0	27398	0	0
$x^4-x^3-4x^2+4x+1$	256400	0	0	0	0	0	0
$x^4+x^3-4x^2-4x+1$	0	0	261080	0	0	0	0
$x^4-2x^3-2x^2+3x+1$	0	0	0	0	17220	0	0
$x^5+x^4-4x^3-3x^2+3x+1$	141000	0	0	0	0	0	0
$x^5-x^4-4x^3+3x^2+3x-1$	0	0	204100	0	0	0	0
$x^6-5x^4+x^3+6x^2-x-1$	12039	0	0	0	0	0	0
$x^6-5x^4-x^3+6x^2+x-1$	0	0	97958	0	0	0	0
$x^6+x^5-5x^4-4x^3+6x^2+3x-1$	190120	0	0	0	0	0	0
$x^6-x^5-5x^4+4x^3+6x^2-3x-1$	0	0	293970	0	0	0	0
$x^7-x^6-6x^5+5x^4+10x^3-7x^2-4x+3$	0	0	84067	0	0	0	0
$x^7+x^6-6x^5-5x^4+10x^3+7x^2-4x-3$	77216	0	0	0	0	0	0
$\|P_j\|_{I_j}^{1/\partial P_j}$	.99007	.97734	.98863	.96922	.97168	.95048	.95052

Bibliography

[1] Mathpages - http://tinyurl.com/yszxbt, 3 2008.

[2] W. W. Adams and P. Loustaunau. *An introduction to Gröbner bases*, volume 3 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1994.

[3] J. Aguirre, M. Bilbao, and J. C. Peral. The trace of totally positive algebraic integers. *Math. Comp.*, 75(253):385–393 (electronic), 2006.

[4] J. Aguirre and J. C. Peral. The integer Chebyshev constant of Farey intervals. To Appear, 2007.

[5] A. A. Albert. *Fundamental concepts of higher algebra*. The University of Chicago Press, Chicago, Ill., 1958.

[6] F. Amoroso. Sur le diamètre transfini entier d'un intervalle réel. *Ann. Inst. Fourier (Grenoble)*, 40(4):885–911 (1991), 1990.

[7] E A Bernando. Sobre unos sistemas de numeros enteros algebraicos de D.S. Gorshkov y sus applicaciones al calculo. *Revista Matemática Hispanoamericana*, 41:3–17, 1981.

[8] P. B. Borwein and T. Erdélyi. *Polynomials and Polynomial Inequalities*. Springer, New York, NY, 1995.

[9] P. B. Borwein and T. Erdélyi. The integer Chebyshev problem. *Math. Comp.*, 65(214):661–681, 1996.

[10] P. B. Borwein, C. G. Pinner, and I. E. Pritsker. Monic integer Chebyshev problem. *Math. Comp.*, 72(244):1901–1916, 2003.

[11] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1997. An introduction to computational algebraic geometry and commutative algebra.

[12] D. S. Dummit and R. M. Foote. *Abstract Algebra*. John Wiley & Sons, Inc., third edition, 2004.

[13] Moawwad E. A. El-Mikkawy. Explicit inverse of a generalized Vandermonde matrix. *Appl. Math. Comput.*, 146(2-3):643–651, 2003.

[14] M. Fekete. Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten. *Math. Zeit.*, 17:228–249, 1923.

[15] Le Baron O. Ferguson. *Approximation by polynomials with integral coefficients*, volume 17 of *Mathematical Surveys*. American Mathematical Society, Providence, R.I., 1980.

[16] V. Flammang. Sur le diamètre transfini entier d'un intervalle à extrémités rationnelles. *Ann. Inst. Fourier (Grenoble)*, 45(3):779–793, 1995.

[17] V. Flammang. Trace of totally positive algebraic integers and integer transfinite diameter. 2007.

[18] V. Flammang and G. Rhin. Algebraic integers whose conjugates all lie in an ellipse. *Math. Comp.*, 74(252):2007–2015 (electronic), 2005.

[19] V. Flammang, G. Rhin, and J.-M. Sac-Épée. Integer transfinite diameter and polynomials with small Mahler measure. *Math. Comp.*, 75(255):1527–1540 (electronic), 2006.

[20] V. Flammang, G. Rhin, and C. J. Smyth. The integer transfinite diameter of intervals and totally real algebraic integers. *J. Théor. Nombres Bordeaux*, 9(1):137–168, 1997.

[21] W. Fulton. *Algebraic Curves*. W.A. Benjamin, Inc., New York, NY, 1969.

[22] G. M. Golusin. *Geometrische Funktionentheorie*. Hochschulbücher für Mathematik, Bd. 31. VEB Deutscher Verlag der Wissenschaften, Berlin, 1957.

[23] D. S. Gorškov. On the distance from zero on the interval $[0,1]$ of polynomials with integral coefficients (russian). In *Proceedings of the Third All Union Mathematical Congress (Moscow 1956)*, volume 4, pages 5–7. Akad. Nauk. SSSR, 1959.

[24] L. Habsieger and B. Salvy. On integer Chebyshev polynomials. *Math. Comp.*, 66(218):763–770, 1997.

[25] K.G. Hare. Generalized Gorshkov-Wirsing polynomials. To Appear.

[26] K.G. Hare. List of polynomials with small normalised leading coefficients. Personal communication, 10 2007.

[27] K.G. Hare and C.J. Smyth. The monic integer transfinite diameter. *Math. Comp.*, 75:1997–2019, 2006.

[28] K.G. Hare and C.J. Smyth. Corrigendum to "The monic integer transfinite diameter". *Math. Comp.*, 2007.

[29] D. Hilbert. Ein Beitrag zur Theorie des Legendre'schen Polynoms. *Acta Math.*, 18(1):155–159, 1894.

[30] J. Hilmar. Consequences of the continuity of the monic integer transfinite diameter. In J. McKee and C.J. Smyth, editors, *Number Theory and Polynomials*, 2007.

[31] J. Hilmar. http://www.cyclotomic.org.uk/research/research.html, 11 2007.

[32] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261(4):515–534, 1982.

[33] Maplesoft. Maple v.11.02, 2007.

[34] The MathWorks. Matlab v.7.4.0.336, 2007.

[35] H. L. Montgomery. *Ten Lectures on the Interface between Analytic Number Theory and Harmonic Analysis*, volume 84 of *CBMS Regional Conference Series in Mathematics*. AMS, 1994.

[36] G. Pólya and G. Szegö. *Aufgaben und Lehrsätze aus der Analysis*, volume 1. Springer Verlag, third edition, 1964.

[37] W. H. Press, B. P. Flannery, S. A. Teukolsky, and W. T. Vetterling. *Numerical recipes*. Cambridge University Press, Cambridge, 1986. The art of scientific computing.

[38] I. E. Pritsker. Small polynomials with integer coefficients. (To Appear), 2005.

[39] R. M. Robinson. Intervals containing infinitely many sets of conjugate algebraic integers. In *Studies in mathematical analysis and related topics*, pages 305–315. Stanford Univ. Press, Stanford, Calif., 1962.

[40] B. C. Roy and A. K. Choudhury. On the determination of the inverse of a Vandermonde matrix. *Internat. J. Control (1)*, 12:525–527, 1970.

[41] E. B. Saff and R. S. Varga. On lacunary incomplete polynomials. *Math. Z.*, 177(3):297–314, 1981.

[42] C. J. Smyth. On the measure of totally real algebraic integers. *J. Austral. Math. Soc. Ser. A*, 30(2):137–149, 1980/81.

[43] C. J. Smyth. On the measure of totally real algebraic integers. II. *Math. Comp.*, 37(155):205–208, 1981.

[44] C. J. Smyth. The mean values of totally real algebraic integers. *Math. Comp.*, 42(166):663–681, 1984.

[45] Q. Wu. On the linear independence measure of logarithms of rational numbers. *Math. Comp.*, 72(242):901–911 (electronic), 2003.